Cisco IOS Interface and Hardware Component Command Reference

First Published: 2014-08-07

Last Modified: 2023-10-05

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

A through B

1pps

To configure the pulse per second parameters of the global navigation satellite system (GNSS) module on the Cisco ASR 903, Cisco ASR 907, and the Cisco ASR 920 routers, use the **1pps** command in the gnss mode. To remove the 1pps configuration, use the **no** form of this command.

1pps {**offset** | **polarity [negative]**}
no 1pps {**offset** | **polarity negative**}

Syntax Description

offset	Configures the 1PPS cable compensation. The valid values are from 0 to 1000 nano seconds.
polarity	Configures the 1PPS polarity.
negative	Configures the polarity as negative. Default polarity is positive.

Command Default

No default behavior or values.

Command Modes

GNSS configuration (config-gnss)

Command History

Release	Modification
IOS-XE 3.17	This command was introduced on the Cisco ASR 903, Cisco ASR 907, and the Cisco ASR 920 routers.

Usage Guidelines

The pulse per second is used to synchronize time with other sensors and is crucial for the accuracy of the sensor integration.

Examples

The following example shows how to configure the PPS:

```
Router# configure terminal
Router(config)# gnss slot r0
Router(config-gnss)# 1pps polarity negative
```

Related Commands

Command	Description
gnss	Configures the GNSS on the router.
anti-jam	Enables or disables the anti-jam mode on the GNSS module.
constellation	Configures the GNSS module based on the specified satellite constellations.
default	Resets the device to its default state.
exit	Exists the GNSS sub mode.
no	Negates the command or sets the value of the command to its default values.
shutdown	Enables GNSS module.

ais-core-failure

To enable AIS alarms to detect core failure events on a 8/16 T1E1 IM, use the ais-core-failure command in controller configuration mode. To disable the AIS alarms, use the no form of this command..

ais-core-failure

no ais-core-failure

Syntax Description

Syntax Description

This command has no keywords or arguments.

Command Default

This command is disabled by default; AIS alarm is not reported during core failure events.

Command Modes

Controller configuration

Command History

Release	Modification
IOS XE Everest 16.7.1	Support for this command was introduced on the Cisco ASR 900 Routers.

Usage Guidelines

AIS alarms are generated and detected either when the TDM circuits goes down on the access layer of the network topology or a failure occurs in the MPLS domain due to which SAToP connectivity goes down. This alarm is only applicable for SDH-E1 and unframed (SAToP) type and is not applicable for framed (CESoP) type.

You cannot configure AIS alarms if CEM group is enabled.You must first remove the CEM group configuration and then configure AIS alarms.

Examples

The following example shows the configuration of AIS alarm:

```
Router> enable
Router#configure terminal
Router(config)#controller t1 0/1/2
Router(config-controller)#ais-core-failure
```

Related Commands

Command	Description
show run | sec	Displays the AIS alarm configuration.

ais-shut

To enable automatic insertion of a Line Alarm Indication Signal (LAIS) in the sent SONET signal whenever the SONET port enters the administrative shutdown state, use the **ais-shut** command in SONET configuration mode. To disable automatic insertion of a LAIS, use the **no** form of this command..

ais-shut

no ais-shut

Syntax Description

Syntax Description

This command has no keywords or arguments.

Command Default

This command is disabled by default; no AIS is sent.

Command Modes

Controller configuration

Command History

Release	Modification
XE 3.18 SP	Support for this command was introduced on NCS 4200 Series.

Usage Guidelines

When the line is placed in administrative shutdown state, use the **ais-shut** command to send a signal to downstream equipment that indicates that there is a problem with the line.

Examples

The following example shows the configuration of AIS SHUT:

```
enable
configure terminal
controller MediaType 0/5/0
mode sonet
controller sonet 0/5/0
ais-shut
end
```

Related Commands

Command	Description
controller sonet	Configures the SONET mode.
show controller sonet	Displays SONET controller configuration.

alarm-interface

To enter alarm-interface mode and configure the alarm interface controller (AIC), use the **alarm-interface** command in global configuration mode. To leave alarm-interface mode, use the **exit** command.

alarm-interface *slot-number*

Syntax Description

slot-number	Number of the port in which the AIC is installed.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)XG	This command was introduced for the Cisco 2600 series and the Cisco 3600 series.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Examples

The following examples show how the **alarm-interface** command is used in conjunction with the **ipaddress** and the **reset** commands:

```
Router(config)# alarm-interface 5
Router(config-aic)# ip address 10.2.130.105
```

A change in the AIC IP configuration might not take effect until the next time the card is started. Use the **reset** command to restart the card, as in the following example:

```
Router(config-aic)# reset
Alarm Interface Card in slot 5 restarted
Router(config-aic)# end
```

Related Commands

Command	Description
ip address	Sets a primary or secondary IP address for an interface.
reset	Resets the AIC CPU.

alarm-profile

To create an alarm profile for chassis, card or interface module, and port, use the **alarm-profile** command in configuration mode. To delete the alarm profile, use the **no** form of this command.

The alarm profile is associated to an alarm with controller types such as SONET, SDH, DS1, or DS3.

alarm-profile *profile-name* {**chassis** | **card** | **port**}

Syntax Description

Syntax Description

profile-name	The name of the alarm profile. The name should be a string with alpha numeric characters and should not exceed 32 characters.
chassis	Alarm profile created for chassis.
card	Alarm profile created for card.
port	Alarm profile created for port.

Command Default

None

Command Modes

Configuration mode

Command History

Release	Modification
Cisco IOS XE 16.8.1	Support for this command was introduced on ASR 900 Series.

Usage Guidelines

This command is used to create alarm profile for chassis, card, or port in the configuration mode.

Examples

The following example shows how to create an alarm profile for chassis:

```
router(config)#alarm profile CHASSIS chassis
router(config-alarm-profile)#alarm sonet/sdh
router(config-alarm-properties)#SLOF syslog
router(config-alarm-properties)#SLOF severity critical
```

Examples

The following example shows how to create an alarm profile for card:

```
 router(config)#alarm profile CARD card
router(config-alarm-profile)#alarm ds3
router(config-alarm-properties)#DS3_RX_LOS syslog
router(config-alarm-properties)#DS3_RX_LOS severity major
```

Examples

The following example shows how to create an alarm profile for port:

```
 router(config)#alarm profile PORT port
router(config-alarm-profile)#alarm ds1
router(config-alarm-properties)#DS1_LOS syslog
router(config-alarm-properties)#DS1_LOS severity major
```

Related Commands

Command	Description
alarm-profile *name***attach**	Attaches alarm profile to chassis or card.
attach profile *profile-name*	Attaches alarm profile to port.
show alarm-profile	Displays alarm profile configured for chassis.

alarm-profile attach

To attach an alarm profile to chassis or card, use the **alarm-profile** *name* **attach** command in configuration mode. To detach the alarm profile from chassis or card, use the **no** form of this command.

After attaching the alarm profile only, the alarm serverity and other alarm functionalities are applied to the chassis, card, or port.

alarm-profile *profile-name* attach {**chassis** | **card** *slot/bay*}

alarm-profile *telcordia* **attachchassis**

Syntax Description

Syntax Description

profile-name	The name of the alarm profile.
chassis	Specify to attach the alarm profile to chassis.
card *slot/bay*	Specify to attach the alarm profile to card.
telcordia	Specify to attach the Telcordia alarm profile to chassis.

Command Default

None

Command Modes

Configuration mode

Command History

Release	Modification
Cisco IOS XE 16.8.1	Support for this command was introduced on ASR 900 Series.
Cisco IOS XE 17.3.1	Support for attaching the Telcordia alarm profile to chassis was introduced.

Usage Guidelines

This command is used to attach alarm profile to chassis or card in the configuration mode.

For Telcordia alarm profile, the alarm severities Not Alarmed (NA) and Not Reported (NR) are included by default. The alarm profile attached to chassis inherits the alarm severities of the Telcordia profile.

Note Ensure that you use the complete **`alarm-profile telcordia attach chassis`** command while attaching the alarm profile based on Telcordia.

Examples

The following example shows how to attach an alarm profile for chassis:

```
 router>enable
router#configure terminal
router(config)#alarm-profile CHASSIS attach chassis
router(config)#end
```

Examples

The following example shows how to attach a Telcordia alarm profile to chassis:

```
 router>enable
router#configure terminal
router(config)#alarm-profile telcordia attach chassis
router(config)#end
```

Examples

The following example shows how to attach an alarm profile to card:

```
 router>enable
router#configure terminal
router(config)#alarm-profile CARD attach card 0/1
router(config)#end
```

Related Commands

Command	Description
alarm-profile *profile-name*	Creates a new alarm profile for chassis, card or port.
show alarm-profile	Displays alarm profile configured for chassis.

alarm report all

To permit selected SONET alarms to be logged to the console for a SONET controller, use the **alarm report all** command in SONET configuration mode. To disable logging of select SONET alarms, use the **no** form of this command.

alarm-report all {*b1-tca* | *lias* | *lrdi* | *pais* | *plop* | *pplm* | *pplm* | *prdi* | *sd-ber*}

Syntax Description

Syntax Description

b1-tca	The name of a CEM interface parameters class.
lias	Reports Line Alarm Indication signal (LAIS) errors.
lrdi	Reports line remote defect indication errors.
pais	Enables reporting of Path Alarm Indication Signal (PAIS).
plop	Enables reporting of Path Loss Of Pointer (PLOP).
pplm	Sets Path Payload Mismatch (PPLM) defect reporting status.
prdi	Sets Path Remote Defect Indication (PRDI) reporting status.
sd-ber	Enables Signal Degrade (SD) Bit Error Rate (BER) reporting.

Command Default

None

Command Modes

Controller configuration

Command History

Release	Modification
XE 3.18 SP	Support for this command was introduced on NCS 4200 Series.

Usage Guidelines

This command is used to configure the alarm reports in SONET mode.

Examples

The following example shows the configuration of alarm reports:

```
enable
configure terminal
controller MediaType 0/5/0
mode sonet
controller sonet 0/5/0
alarm report all b1-tcs
end
```

Related Commands

Command	Description
controller sonet	Configures the SONET mode.

Command	Description
show controller sonet	Displays SONET controller configuration.

als

To enable the Automatic Laser Shutdown (ALS) mode, use the **als**command in interface configuration mode. To disable ALS mode, use the no form of this command.

als
no als

Syntax Description

This command has no arguments or keywords.

Command Default

ALS is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SRD1	This command was introduced on the Cisco 7600 series router for the ES+ line cards.

Examples

The following example shows how to enable ALS:

```
Router> enable
Router# configure terminal
Router(config)# interface tengigabitethernet 2/1
Router(config-if)# als
```

Related Commands

Command	Description
als restart	Requests an ALS restart mode.
als restart mode	Selects the ALS restart mode.
als restart pulse	Select the ALS pulse mode.
hw-module als restart	Requests a restart pulse.
show als	Displays ALS status.

als restart

To request an Automatic Laser Shutdown (ALS) restart mode, use the **alsrestart**command in interface configuration mode. To disable an ALS restart mode, use the no form of this command.

als restart {**mode** | **pulse**}
no als restart {**mode** | **pulse**}

Syntax Description

mode	Specifies the ALS mode.
pulse	Specifies the ALS pulse.

Command Default

Command default is automatic.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SRD1	This command was introduced on the Cisco 7600 series router for the ES+ line cards.

Examples

The following example restarts the ALS mode:

```
Router> enable
Router# configure terminal
Router(config)# interface tengigabitethernet 2/1
Router(config-if)# als
Router(config-if)# als restart mode
```

Related Commands

Command	Description
als	Enables the ALS mode.
als restart mode	Selects the ALS restart mode.
als restart pulse	Selects the ALS pulse mode.
hw-module als restart	Requests a restart pulse.
show als	Displays ALS status.

als restart mode

To select the Automatic Laser Shutdown (ALS) restart mode, use the **alsrestartmode**command in interface configuration mode. To reset to the command default mode, use the no form of this command.

als restart mode {**automatic** | **manual**}
no als restart mode {**automatic** | **manual**}

Syntax Description

automatic	Selects automatic mode.
manual	Selects manual mode.

Command Default

Command default is automatic.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SRD1	This command was introduced on the Cisco 7600 series router for the ES+ line cards.

Usage Guidelines

In manual restart, you request a single restart pulse from the ALS agent. In automatic restart, you configure the ALS agent to send a periodic restart pulse.

Examples

The following example shows how to select automatic mode:

```
Router> enable
Router# configure terminal
Router(config)# interface tengigabitethernet 2/1
Router(config-if)# als
Router(config-if)# als restart mode automatic
```

Related Commands

Command	Description
als	Enables the ALS mode.
als restart	Requests an ALS restart mode.
als restart pulse	Select the ALS pulse mode.
hw-module als restart	Requests a restart pulse.
show als	Displays ALS status.

als restart pulse

To select the Automatic Laser Shutdown (ALS) pulse mode, use the **alsrestartpulse**command in inteface configuration mode. To disable an ALS pulse mode, use the no form of this command.

als restart pulse {**interval** **seconds** | **width** **seconds**}
no als restart pulse {**interval** **seconds** | **width** **seconds**}

Syntax Description

interval **seconds**	Specifies the interval of the ALS pulse. The range is 100 to 20,000 seconds. Default is 300 seconds.
width seconds	Specifies the width of the ALS pulse. The range is 2 to 200 seconds. Default is 200 seconds.

Command Default

Pulse interval default is 300 seconds. Pulse width default is 200 seconds.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SRD1	This command was introduced on the Cisco 7600 series router for the ES+ line cards.

Usage Guidelines

If a particular platform/OS/interface/controller has the capability to support two ranges, one range for Wave Division Multiplexing (WDM) and another for non-WDM, use the following pulse width ranges:

- WDM: 60 - 200 (default: 100)
- Non-WDM: 2 - 100 (default: 4)

The recovery pulse interval is the period between the rising edge of pulses. The pulse interval needs to be greater than the pulse width. If a particular platform/OS/interface/controller has the capability to support two ranges, one range for WDM and another for non-WDM, use the following pulse width ranges:

- WDM: 200 - 20000 (default: 300)
- Non-WDM: 100 - 2000 (default: 100)

Examples

The following example shows how to select an ALS pulse interval:

```
Router> enable
Router# configure terminal
Router(config)# interface tengigabitethernet 2/1
Router(config-if)# als
Router(config-if)# als restart mode
Router(config-if)# als restart mode automatic
Router(config-if)# als restart pulse interval 2000
```

The following example shows how to select an ALS pulse width:

```
Router> enable
Router# configure terminal
```

```
Router(config)# interface tengigabitethernet 2/1
Router(config-if)# als
Router(config-if)# als restart mode
Router(config-if)# als restart mode automatic
Router(config-if)# als restart pulse width 200
```

Related Commands

Command	Description
als	Enables the ALS mode.
als restart	Requests an ALS restart mode.
als restart mode	Selects the ALS restart mode.
hw-module als restart	Requests a restart pulse.
show als	Displays ALS status.

analysis-module monitoring

To enable Network Analysis Module (NAM) packet monitoring on an interface, use the **analysis-modulemonitoring** command in interface configuration mode. To disable NAM packet monitoring, use the **no** form of this command.

analysis-modulemonitoring
noanalysis-modulemonitoring

Syntax Description

This command has no arguments or keywords.

Command Default

NAM packet monitoring is disabled on the interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced on the following platforms: Cisco 2600XM series, Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.3(8)T4	This command was implemented on the following platforms: Cisco 2811, Cisco 2821, Cisco 2851, and Cisco 3800 series.
12.3(11)T	This command was implemented on the Cisco 3800 series.
Cisco IOS XE Fuji 16.9.1	This command was implemented on the Cisco ISR 4000 Series Integrated Services Routers.

Usage Guidelines

When you enable NAM packet monitoring on an interface, Cisco Express Forwarding (CEF) sends an extra copy of IP packet that is received or sent on that interface to the NAM through the analysis module and then through the internal NM-NAM interface.

Note The traffic is sent through the internal NAM interface and through the the analysis module interface uses the router's resources such as CPU, SDRAM bandwidth, and backplane Peripheral Component Interconnect (PCI) bandwidth. Therefore, it is recommended to use the internal NAM interface to monitor WAN interfaces and use the external NAM interface to monitor LAN interfaces.

In Cisco IOS XE Fuji 16.9.1, Encapsulated Remote Switched Port Analyzer (ERSPAN) supports the NAM feature on Cisco 4000 Series ISRs. The Cisco ERSPAN feature allows you to monitor traffic on one or more ports and then sends the monitored traffic to one or more destination ports.

To enhance the performance of NAM and simplify the configuration of NAM data port, ERSPAN sessions are extended to a special souce session called NAM SPAN. NAM SPAN supports Layer 2 mode as local span and monitors the interface on Layer 3 interface on Cisco 4000 Series ISRs.

Note If an interface is monitored by NAM SPAN, it can not be configured as output interface. Each interface can configure only one interface as output interface.

Examples

The following example shows how to enable NAM packet monitoring on a serial interface:

```
Router(config)# interface serial 0/0
Router(config-if)# analysis-module monitoring
```

The following example shows how to enable NAM packet monitoring on a serial interface of a Cisco 4000 Series ISRs:

```
Router(config)# interface serial 0/0
Router(config-if)# analysis-module monitoring ucse0/0/0
```

Note The output interface is ucse0/0/0 which is configured as NAM/vNAM data port and the source interface is serial 0/0 in this example.

announce interval

To set an interval value for timing announcement packets, use the **announceinterval** command in Precision Time Protocol clock port mode. To remove an announcement interval configuration, use the **no** form of this command.

announce interval *interval-value*
no announce interval *interval-value*

Syntax Description

interval-value	Specifies the interval for announce messages. The intervals use log base 2 values, as follows: • 4--1 packet every 16 seconds • 3--1 packet every 8 seconds • 2--1 packet every 4 seconds • 1--1 packet every 2 seconds • 0--1 packet every second

Command Default

For the IE 3000 switch, the default value is 1. For the MWR 2941 router, the default value is 2.

Command Modes

PTP clock port configuration (config-ptp-port)

Command History

Release	Modification
15.0(1)S	This command was introduced.

Usage Guidelines

The interval value defined by this command impacts the timeout value defined by the **announcetimeout** command.

Examples

The following example shows how to configure an announcement interval:

```
Router# configure terminal
Router(config)# ptp clock ordinary domain 0
Router(config-ptp-clk)# clock-port slave slaveport
Router(config-ptp-port)# announce interval 3
Router(config-ptp-port)# end
```

Related Commands

Command	Description
announce timeout	Sets the timeout value for timing announcement packets.

announce timeout

To set a timeout value for timing announcement packets, use the **announcetimeout** command in Precision Time Protocol clock port mode. To remove an announcement timeout configuration, use the **no** form of this command.

announce timeout *timeout-value*
no announce timeout *timeout-value*

Syntax Description

timeout-value	Specifies the number of announcement intervals before the session times out. The range is from 1 to 10. The default is 3.

Command Default

The default timeout value is 3.

Command Modes

PTP clock port configuration (config-ptp-port)

Command History

Release	Modification
15.0(1)S	This command was introduced.

Usage Guidelines

This command configures the number of announcement intervals before the session times out. To define the length of the announcement intervals, use the **announceinterval** command.

Examples

The following example shows how to configure an **announcementtimeout**:

```
Device> enable
Device# configure terminal
Device(config)# ptp clock ordinary domain 0
Device(config-ptp-clk)# clock-port slave slaveport
Device(config-ptp-port)# announce timeout 7
Device(config-ptp-port)# end
```

Related Commands

Command	Description
announce interval	Sets interval value for timing announcement packets.

anti-jam

To configure the anti-jam mode for the GNSS module on the Cisco ASR 903, Cisco ASR 907, and the Cisco ASR 920 routers, use the **anti-jam** command in gnss mode.

anti-jam disable

Syntax Description

disable	Disables the anti-jam mode.

Command Default

Anti-jam is enabled on the GNSS module by default.

Command Modes

GNSS configuration (config-gnss)

Command History

Release	Modification
IOS-XE 3.17	This command was introduced on the Cisco ASR 903, Cisco ASR 907, and the Cisco ASR 920 routers.

Examples

The following example shows how to disable the anti-jam mode on the GNSS module:

```
Router# configure terminal
Router(config)# gnss slot r0
Router(config-gnss)# anti-jam disable
```

Related Commands

Command	Description
gnss	Configures the GNSS on the router.
1pps	Configures the pulse per second from the GNSS module.
constellation	Configures the GNSS module based on the specified satellite constellations.
default	Resets the device to its default state.
exit	Exists the GNSS sub mode.

apply (satellite initial configuration)

To save new or changed satellite initial configuration parameters and to reset the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT), use the **apply** command in satellite initial configuration mode.

apply

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Satellite initial configuration mode

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The **apply** command saves any new or changed satellite initial configuration parameters to the nonvolatile memory of the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT) and initiates a network module software reset. Commands entered in satellite initial configuration mode do not appear in the router configuration.

When you enter the **exit** or **end** command to exit satellite initial configuration mode, the system automatically saves any changed parameters to the NM-1VSAT-GILAT network module's nonvolatile memory and resets the NM-1VSAT-GILAT network module.

Note This command is typically used by an installation technician. Do not use this command unless your satellite service provider instructs you to perform the satellite initial configuration and provides all necessary parameter values.

Examples

The following example shows what appears when you enter the **apply** command after changing some initial configuration parameters:

```
Router(sat-init-config)# apply

Applying changed parameters to the satellite module.
Parameter update succeeded.  Module is now resetting.
Router(sat-init-config)#
```

The following example shows what appears when you enter the **apply** command when no parameters have been changed:

```
Router(sat-init-config)# apply

% No new or changed parameters to apply.
Router(sat-init-config)#
```

Related Commands

Command	Description
end (satellite initial configuration)	Exits satellite initial configuration mode, saves any new or changed parameters, and resets the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT).
exit (satellite initial configuration)	Exits satellite initial configuration mode, saves any new or changed parameters, and resets the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT).

aps authenticate

To enable authentication and specify the string that must be present to accept any packet on the out-of-band (OOB) communications channel on a Packet-over-SONET (POS) interface, use the **apsauthenticate** command in interface configuration mode. To disable authentication, use the **no** form of this command.

aps authenticate *string*
no aps authenticate

Syntax Description

string	Text that must be present to accept the packet on a protected or working interface. A maximum of eight alphanumeric characters are accepted.

Command Default

Authentication is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.1CC	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **apsauthenticate**command to ensure that only valid packets are accepted on the OOB communications channel.

The **apsauthenticate** command must be configured on both the working and protect interfaces.

Examples

The following example shows how to enable authentication on POS interface 0 in slot 4:

```
Router# configure terminal
Router(config)# interface pos 4/0/0
Router(config-if)# aps working 1
Router(config-if)# aps authenticate sanjose
Router(config-if)# end
```

Related Commands

Command	Description
aps protect	Enables a POS interface as a protect interface.
aps working	Configures a POS interface as a working interface.

aps adm

Use this command to configure unidirectional ACR (SONET Framing).

aps adm *slot* / *bay* / *port*

Syntax Description

Syntax Description

There are no keywords for this command.

Command Default

None

Command Modes

Controller configuration

Command History

Release	Modification
XE 3.18 SP	Support for this command was introduced on NCS 4200 Series.

Usage Guidelines

The command is used to enable Add Drop Multiplexer (ADM) with unidirectional APS protection.

Examples

The following example shows how to configure unidirectional ACR (SONET Framing):

```
enable
configure terminal
controller MediaType 0/5/0
mode sonet
controller sonet 0/5/0
clock source internal
aps group acr 1
aps working 1
aps unidirectional
aps adm
exit
controller sonet 0/5/0
aps group acr 1
aps protect 1 10.7.7.7
aps revert 3
end
```

Related Commands

Command	Description
controller sonet	Configures the SONET mode.
show controller sonet	Displays SONET controller configuration.

aps clear sonet

To remove all externally initiated SONET automatic protection switching (APS) commands configured on a Cisco AS5850, use the **apsclearsonet**command in privileged EXEC mode.

aps clear sonet *slot*/*port*

Syntax Description

slot	Slot number on an STM-1 trunk card.
/ *port*	SONET port number on an STM-1 trunk card. The slash mark is required between the *slot* argument and the *port* argument.

Command Default

No APS switch commands are removed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(11)T	This command was introduced on the Cisco AS5850.

Usage Guidelines

Use the **apsclearsonet**command to remove any SONET APS commands, such as the **apsforcesonet**command, that could switch the working fiber to the protect fiber on an STM-1 trunk card.

This command applies to the Cisco AS5850 universal gateway only.

Examples

The following example shows how to remove all externally initiated SONET APS switch commands:

```
Router# aps clear sonet 1/0
```

Related Commands

Command	Description
aps force sonet	Requests an APS forced switch of a specified port to the alternate port unless a request of equal or higher priority is in effect.
aps lockout sonet	Prevents a working SONET port from switching to a protect SONET port unless a request of equal or higher priority is in effect.
aps manual sonet	Requests a manual APS switch on a SONET port.
aps protect (SONET)	Enables SONET APS.

aps force

To manually switch the specified circuit to a protect interface, unless a request of equal or higher priority is in effect, use the **apsforce**command in interface configuration mode. To cancel the switch, use the **no** form of this command.

aps force *circuit-number*
no aps force *circuit-number*

Syntax Description

circuit-number	Number of the circuit to switch to the protect interface.

Command Default

No circuit is switched.

Command Modes

Interface configuration

Command History

Release	Modification
11.1CC	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **apsforce**command to manually switch the interface to a protect interface when you are not using the **apsrevert**command. For example, if you need to change the fiber connection, you can manually force the working interface to switch to the protect interface.

In a one-plus-one (1+1) configuration only, you can use the **apsforce0** command to force traffic from the protect interface back onto the working interface.

The**apsforce** command has a higher priority than any of the signal failures or the **apsmanual** command.

The **apsforce** command is configured only on protect interfaces.

Examples

The following example shows how to force the circuit on POS interface 0 in slot 3 (a protect interface) back onto a working interface:

```
Router# configure terminal
Router(config)# interface pos 3/0/0
Router(config-if)# aps protect 10/30/1/1
Router(config-if)# aps force 1
Router(config-if)# end
```

Related Commands

Command	Description
aps manual	Manually switches a circuit to a protect interface.
aps protect	Enables a POS interface as a protect interface.

Command	Description
aps working	Configures a POS interface as a working interface.

aps force sonet

To force a specified port to switch to the alternate port within a redundant pair unless a request of equal or higher priority is in effect, use the **apsforcesonet**command in privileged EXEC mode.

aps force sonet *slot/port* **from** {**protection** | **working**}

Syntax Description

slot	Slot number on an STM-1 trunk card.
/ *port*	SONET port number on an STM-1 trunk card. The slash mark is required between the *slot* argument and the *port* argument.
from protection	Specifies that you want to switch from the protect port to the working port.
from working	Specifies that you want to switch from the working port to the protect port.

Command Default

No port is switched.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(11)T	This command was introduced on the Cisco AS5850.

Usage Guidelines

Forced is a defined APS request priority level. The request succeeds if no higher priority request (lockout is the only higher priority request) is posted. The **apsforcesonet**command does not persist after a system restart. The *slot* and *port* arguments indicate the SONET interface on which you want to issue the **apsforcesonet** command. The**apsforcesonet** command has a higher priority than any of the signal failures or the **apsmanualsonet** command.

For more information about APS priority requests, see the ITU-T G.841 standard.

This command applies to the Cisco AS5850 universal gateway only.

Examples

The following example shows how to force the protect port in the SONET controller to become an active port:

```
Router# configure terminal
Router(config)# controller sonet 1/0
Router(config-controller)# aps protect
Router(config-controller)# end
Router# aps force sonet 1/0 from working
```

Related Commands

Command	Description
aps clear sonet	Removes any APS switch commands configured using CLI.
aps lockout sonet	Prevents a working SONET port from switching to a protect SONET port unless a request of equal or higher priority is in effect.

Command	Description
aps manual sonet	Requests a manual APS switch on a SONET port.
aps protect (SONET)	Enables SONET APS.

aps group

To allow more than one protect and working interface and Access Circuit Redundancy (ACR) group to be supported on a router, use the **aps group** command in interface configuration or controller configuration mode. To remove a group, use the **no** form of this command.

aps group [**acr**] *group-number*
no aps group [**acr**] *group-number*

Syntax Description

acr	(Optional) Specifies an ACR group.
group-number	Number of the group. The default is 0.

Command Default

No groups exist.

Note 0 is a valid group number.

Command Modes

Interface configuration (config-if)
Controller configuration (config-controller)

Command History

Release	Modification
11.1CC	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(1)S	This command was modified. The **acr** keyword was added.

Usage Guidelines

Use the **aps group**command to specify more than one working and protect interface on a router--for example, working channel for group 0 and protect channel for group 1 on one router, and working channel for group 1 and protect channel for group 0 on another router.

The default group number is 0. The **aps group 0** command does not imply that no groups exist.

The **aps group** command must be configured on both the protect and working interfaces.

Use the **acr**keyword to configure an ACR working or protect interface.

Examples

The following example shows how to configure two working/protect interface pairs. Working interface (3/0/0) is configured in group 10 (the protect interface for this working interface is configured on another router), and protect interface (2/0/1) is configured in group 20.

```
Router# configure terminal
Router(config)# interface ethernet 0/0
```

```
Router(config-if)# ip address 10.7.7.6 255.255.255.0
Router(config-if)# exit
Router(config)# interface pos 3/0/0
Router(config-if)# aps group 10
Router(config-if)# aps working 1
Router(config-if)# exit
Router(config)# interface pos 2/0/1
Router(config-if)# aps group 20
Router(config-if)# aps protect 1 10.7.7.7
Router(config-if)# end
```

On the second router, protect interface (4/0/0) is configured in group 10, and working interface (5/0/0) is configured in group 20 (the protect interface for this working interface is configured on another router).

```
Router(config)# interface ethernet 0/0
Router(config-if)# ip address 10.7.7.7 255.255.255.0
Router(config-if)# exit
Router(config)# interface pos 4/0/0
Router(config-if)# aps group 10
Router(config-if)# aps protect 1 10.7.7.6
Router(config-if)# exit
Router(config)# interface pos 5/0/0
Router(config-if)# aps group 20
Router(config-if)# aps working 1
Router(config-if)# end
```

Related Commands

Command	Description
aps protect	Enables a POS interface as a protect interface.
aps working	Configures a POS interface as a working interface.

aps hspw-icrm-grp

To associate an Automatic Protection Switching (APS) group to an Interchassis Redundancy Manager (ICRM) group number, use the **aps hspw-icrm-grp** command in controller configuration mode. To remove the association, use the **no** form of this command.

aps hspw-icrm-grp *group-number*
no aps hspw-icrm-grp *group-number*

Syntax Description

group-number	ICRM group number. Valid values are from 1 to 4294967295.

Command Default

Interface connections do not switch from one circuit to another if a circuit fails.

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
Cisco IOS 15.2(1)S	This command was introduced.
Cisco IOS XE 3.11S	This command was integrated into Cisco IOS XE Release 3.11S.

Usage Guidelines

Use the **aps hspw-icrm-grp** command to protect SONET networks by enabling SONET connections to switch to another SONET circuit when a circuit failure occurs.

A protect interface serves as the backup interface for the working interface. When the working interface fails, the protect interface quickly assumes the former's traffic load.

Examples

The following example shows how to configure the Multi Router Automatic Protection Switching (MR-APS) integration with HSPW on a Circuit Emulation (CEM) interface on the working router with framing mode as SONET on router P1:

```
RouterP1> enable
RouterP1# configure terminal
RouterP1(config)# pseudowire-class hspw_aps
RouterP1(config-pw-class)# encapsulation mpls
RouterP1(config-pw-class)# status peer topology dual-homed
RouterP1(config-pw-class)# exit
RouterP1(config)# redundancy
RouterP1(config-red)# interchassis group 1
RouterP1(config-r-ic)# member ip 10.2.0.2
RouterP1(config-r-ic)# backbone interface GigabitEthernet 0/1/0
RouterP1(config-r-ic)# backbone interface GigabitEthernet 0/1/1
RouterP1(config-r-ic)# exit
RouterP1(config)# controller SONET 0/1/0
RouterP1(config-controller)# framing sonet
RouterP1(config-controller)# clock source line
RouterP1(config-controller)# sts-1 1
RouterP1(config-ctrlr-sts1)# mode vt-15
RouterP1(config-ctrlr-sts1)# vtg 1 t1 1 cem-group 0 timeslots 1-24
RouterP1(config-ctrlr-sts1)# exit
RouterP1(config-controller)# aps group 3
RouterP1(config-controller)# aps working 1
```

```
RouterP1(config-controller)# aps hspw-icrm-grp 1
RouterP1(config-controller)# exit
RouterP1(config)# interface cem 0/1/0
RouterP1(config-if)# cem 0
RouterP1(config-if)# xconnect 3.3.3.3 1 encapsulation mpls pw-class hspw_aps
RouterP1(config-if)# backup peer 4.4.4.4 2 pw-class hspw_aps
RouterP1(config-if)# exit
RouterP1(config)# end
```

Examples

The following example shows how to configure the MR-APS integration with hot standby pseudowire (HSPW) on a CEM interface on the protect router with framing mode as SONET on router PE1:

```
RouterPE1> enable
RouterPE1# configure terminal
RouterPE1(config)# pseudowire-class hspw_aps
RouterPE1(config-pw-class)# encapsulation mpls
RouterPE1(config-pw-class)# status peer topology dual-homed
RouterPE1(config-pw-class)# exit
RouterPE1(config)# redundancy
RouterPE1(config-red)# interchassis group 1
RouterPE1(config-r-ic)# member ip 10.2.0.1
RouterPE1(config-r-ic)# backbone interface GigabitEthernet 0/1/0
RouterPE1(config-r-ic)# backbone interface GigabitEthernet 0/1/1
RouterPE1(config-r-ic)# exit
RouterPE1(config)# controller SONET 0/2/0
RouterPE1(config-controller)# framing sonet
RouterPE1(config-controller)# clock source line
RouterPE1(config-controller)# sts-1 1
RouterPE1(config-ctrlr-sts1)# mode vt-15
RouterPE1(config-ctrlr-sts1)# vtg 1 t1 1 cem-group 0 timeslots 1-24
RouterPE1(config-ctrlr-sts1)# exit
RouterPE1(config-controller)# aps group 3
RouterPE1(config-controller)# aps protect 1 10.2.0.1
RouterPE1(config-controller)# aps hspw-icrm-grp 1
RouterPE1(config-controller)# exit
RouterPE1(config)# interface cem 0/2/0
RouterPE1(config-if)# cem 0
RouterPE1(config-if)# xconnect 3.3.3.3 3 pw-class hspw_aps
RouterPE1(config-if)# backup peer 4.4.4.4 4 pw-class hspw_aps
RouterPE1(config-if)# exit
RouterPE1(config)# end
```

Examples

The following example shows how to configure the MR-APS integration with HSPW on a CEM interface on the working router with framing mode as SONET on router P2:

```
RouterP2> enable
RouterP2# configure terminal
RouterP2(config)# pseudowire-class hspw_aps
RouterP2(config-pw-class)# encapsulation mpls
RouterP2(config-pw-class)# status peer topology dual-homed
RouterP2(config-pw-class)# exit
RouterP2(config)# redundancy
RouterP2(config-red)# interchassis group 1
RouterP2(config-r-ic)# member ip 10.6.0.2
RouterP2(config-r-ic)# backbone interface GigabitEthernet 0/2/0
RouterP2(config-r-ic)# backbone interface GigabitEthernet 0/2/1
RouterP2(config-r-ic)# exit
RouterP2(config)# controller SONET 0/1/0
RouterP2(config-controller)# framing sonet
```

```
RouterP2(config-controller)# clock source line
RouterP2(config-controller)# sts-1 1
RouterP2(config-ctrlr-sts1)# mode vt-15
RouterP2(config-ctrlr-sts1)# vtg 1 t1 1 cem-group 0 timeslots 1-24
RouterP2(config-ctrlr-sts1)# exit
RouterP2(config-controller)# aps group 3
RouterP2(config-controller)# aps working 1
RouterP2(config-controller)# aps hspw-icrm-grp 1
RouterP2(config-controller)# exit
RouterP2(config)# interface cem 0/1/0
RouterP2(config-if)# cem 0
RouterP2(config-if)# xconnect 1.1.1.1 1 encapsulation mpls pw-class hspw_aps
RouterP2(config-if)# backup peer 2.2.2.2 3 pw-class hspw_aps
RouterP2(config-if)# exit
RouterP2(config)# end
```

Examples

The following example shows how to configure the MR-APS Integration with HSPW on a CEM interface on the protect router with framing mode as SONET on router PE2:

```
RouterPE2> enable
RouterPE2# configure terminal
RouterPE2(config)# pseudowire-class hspw_aps
RouterPE2(config-pw-class)# encapsulation mpls
RouterPE2(config-pw-class)# status peer topology dual-homed
RouterPE2(config-pw-class)# exit
RouterPE2(config)# redundancy
RouterPE2(config-red)# interchassis group 1
RouterPE2(config-r-ic)# member ip 10.6.0.1
RouterPE2(config-r-ic)# backbone interface GigabitEthernet 0/2/0
RouterPE2(config-r-ic)# backbone interface GigabitEthernet 0/2/1
RouterPE2(config-r-ic)# exit
RouterPE2(config)# controller SONET 0/2/0
RouterPE2(config-controller)# framing sonet
RouterPE2(config-controller)# clock source line
RouterPE2(config-controller)# sts-1 1
RouterPE2(config-ctrlr-sts1)# mode vt-15
RouterPE2(config-ctrlr-sts1)# vtg 1 t1 1 cem-group 0 timeslots 1-24
RouterPE2(config-ctrlr-sts1)# exit
RouterPE2(config-controller)# aps group 2
RouterPE2(config-controller)# aps protect 1 10.6.0.1
RouterPE2(config-controller)# aps hspw-icrm-grp 1
RouterPE2(config-controller)# exit
RouterPE2(config)# interface cem 0/2/0
RouterPE2(config-if)# cem 0
RouterPE2(config-if)# xconnect 1.1.1.1 2 pw-class hspw_aps
RouterPE2(config-if)# backup peer 2.2.2.2 4 pw-class hspw_aps
RouterPE2(config-if)# exit
```

Related Commands

Command	Description
aps protect	Configures a POS interface as a protect interface.
aps working	Configures a POS interface as a working interface.

aps lockout

To prevent a working interface from switching to a protect interface, use the **apslockout** command in interface configuration mode. To remove the lockout, use the **no** form of this command.

aps lockout *circuit-number*
no aps lockout *circuit-number*

Syntax Description

circuit-number	Number of the circuit to lock out.

Command Default

No lockout exists.

Command Modes

Interface configuration

Command History

Release	Modification
11.1CC	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **apslockout** command is configured only on protect interfaces.

Examples

The following example shows how to lock out POS interface 3/0/0 (that is, prevents the circuit from switching to a protect interface if the working circuit becomes unavailable):

```
Router# configure terminal
Router(config)# interface pos 3/0/0
Router(config-if)# aps protect 1 10.7.7.7
Router(config-if)# aps lockout 1
Router(config-if)# end
```

Related Commands

Command	Description
aps protect	Enables a POS interface as a protect interface.
aps working	Configures a POS interface as a working interface.

aps lockout sonet

To prevent a working port from switching to a protect port unless a request of equal or higher priority is in effect, use the **apslockoutsonet** command in privileged EXEC mode.

aps lockout sonet *slot/port*

Syntax Description

slot	Slot number on an STM-1 trunk card.
/ *port*	SONET port number on an STM-1 trunk card. The slash mark is required between the *slot* argument and the *port* argument.

Command Default

No lockout exists; that is, a working port is not prevented from switching to a protect port.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(11)T	This command was introduced on the Cisco AS5850.

Usage Guidelines

Lockout is defined as the highest APS request priority level.

The **apslockoutsonet**command does not persist after a system restart. The *slot* and *port* arguments indicate the SONET interface from which the protect port is to be locked out. When the specified port is locked out, SONET APS switching from the working port is not allowed.

For more information about APS priority requests, see the ITU-T G.841 standard.

This command applies to the Cisco AS5850 universal gateway only.

Examples

The following example shows how to lock out SONET port 1/0 (prevents SONET APS switching to a protect interface if the working circuit becomes unavailable):

```
Router# configure terminal
Router(config)# controller sonet 1/0
Router(config-controller)# aps protect
Router(config-controller)# end
Router# aps lockout sonet 1/0
```

Related Commands

Command	Description
aps clear sonet	Removes any APS switch commands configured using CLI.
aps force sonet	Requests an APS forced switch of a specified port to the alternate port unless a request of equal or higher priority is in effect.
aps manual sonet	Requests a manual APS switch on a SONET port.
aps protect (SONET)	Enables SONET APS.

aps manual

To manually switch a circuit to a protect interface, use the **aps manual** command in interface configuration mode. To cancel the switch, use the **no** form of this command.

aps manual *circuit-number*
no aps manual *circuit-number*

Syntax Description

circuit-number	Number of the circuit to switch to a protect interface.

Command Default

No circuit is switched.

Command Modes

Interface configuration

Command History

Release	Modification
11.1CC	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **aps manual** command to manually switch the interface to a protect interface. For example, you can use this feature when you need to perform maintenance on the working channel. If a protection switch is already up, you can also use the **aps manual** command to revert the communication link back to the working interface before the wait to restore (WTR) time has expired. The WTR time period is set by the **aps revert** command.

In a one-plus-one (1+1) configuration only, you can use the **aps manual 0** command to force traffic from the protect interface back onto the working interface.

The**aps manual** command is a lower priority than any of the signal failures or the**aps force** command.

Examples

The following example shows how to force the circuit on POS interface 0 in slot 3 (a working interface) back onto the protect interface:

```
Router# configure terminal
Router(config)# interface pos 3/0/0
Router(config-if)# aps working 1
Router(config-if)# aps manual 1
Router(config-if)# end
```

Related Commands

Command	Description
aps force	Manually switches the specified circuit to a protect interface, unless a request of equal or higher priority is in effect.
aps protect	Enables a POS interface as a protect interface.

Command	Description
aps revert	Enables automatic switchover from the protect interface to the working interface after the working interface becomes available.
aps working	Configures a POS interface as a working interface.

aps manual sonet

To manually switch to the alternate port within a redundant pair unless a request of equal or higher priority is in effect, use the **apsmanualsonet** command in privileged EXEC mode.

aps manual sonet *slot/port* **from** {**protection** | **working**}

Syntax Description

slot	Slot number on an STM-1 trunk card.
/ *port*	SONET port number on an STM-1 trunk card. The slash mark is required between the *slot* argument and the *port* argument.
from protection	Specifies that you want to switch from the protect port to the working port.
from working	Specifies that you want to switch from the working port to the protect port.

Command Default

No port is switched.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(11)T	This command was introduced on the Cisco AS5850.

Usage Guidelines

Use the **apsmanualsonet**command to manually switch the active port to the alternate port. For example, you can use this command when you need to perform maintenance on the working port.

Manual is a defined APS request priority level. The request succeeds if no higher priority request is posted. The **apsmanualsonet**command does not persist after a system restart. The *slot* and *port* arguments indicate the SONET interface on which you want to issue the **apsmanualsonet** command. The**apsmanualsonet** command has a lower priority than any of the signal failures or the **apsforcesonet**command.

For more information about APS priority requests, see the ITU-T G.841 standard.

This command applies to the Cisco AS5850 universal gateway only.

Examples

The following example shows how to manually switch the working port, SONET port 1/0, to the protect port:

```
Router# configure terminal
Router(config)# controller sonet 1/0
Router(config-controller)# aps protect
Router(config-controller)# end
Router# aps manual sonet 1/0 from working
```

Related Commands

Command	Description
aps clear sonet	Removes any APS switch commands configured using CLI.

Command	Description
aps force sonet	Requests an APS forced switch of a specified port to the alternate port unless a request of equal or higher priority is in effect.
aps lockout sonet	Prevents a working SONET port from switching to a protect SONET port unless a request of equal or higher priority is in effect.
aps protect (SONET)	Enables SONET APS.

aps protect

To enable a POS interface as a protect interface, use the **apsprotect**command in interface configuration mode. To remove the POS interface as a protect interface, use the **no** form of this command.

aps protect *circuit-number ip-address*
no aps protect *circuit-number ip-address*

Syntax Description

circuit-number	Number of the circuit to enable as a protect interface.
ip-address	IP address of the router that has the working POS interface.

Command Default

No circuit is protected.

Command Modes

Interface configuration

Command History

Release	Modification
11.1CC	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **apsprotect**command to configure the POS interface used by a working interface if the working interface becomes unavailable because of a router failure, degradation or loss of channel signal, or manual intervention.

Caution Configure the working interface before configuring the protect interface to keep the protect interface from becoming the active circuit and disabling the working circuit when it is finally discovered.

Examples

The following example shows how to configure circuit 1 on POS interface 5/0/0 as a protect interface for the working interface on the router with the IP address of 10.7.7.7. For information on how to configure the working interface, refer to the **apsworking** command.

```
Router# configure terminal
Router(config)# interface pos 5/0/0
Router(config-if)# aps protect 1 10.7.7.7
Router(config-if)# end
```

Related Commands

Command	Description
aps working	Configures a POS interface as a working interface.

aps protect (SONET)

To enable automatic protection switching (APS) on a SONET port in an STM-1 trunk card, use the **apsprotect**command in controller configuration mode. To disable APS on the SONET port, use the **no** form of this command.

aps protect
no aps protect

Syntax Description

This command has no arguments or keywords.

Command Default

APS is disabled.

Command Modes

Controller configuration

Command History

Release	Modification
12.3(11)T	This command was introduced on the Cisco AS5850.

Usage Guidelines

Use the **apsprotect**command to enable APS on a protect SONET port as a working port if the working port becomes unavailable because of a fiber failure, degradation or loss of channel signal, or manual intervention.

Examples

The following example shows how to enable APS on SONET port 0/1 in an STM-1 trunk card.

```
Router# configure terminal
Router(config)# controller sonet 1/0
Router(config-controller)# aps protect
Router(config-controller)# end
```

Related Commands

Command	Description
aps unidirectional	Configures a protect SONET port for unidirectional mode.
show controllers sonet	Displays information about SONET controllers.

aps revert

To enable automatic switchover from the protect interface to the working interface after the working interface becomes available, use the **apsrevert**command in interface configuration mode. To disable automatic switchover, use the **no** form of this command.

aps revert *minutes*
no aps revert

Syntax Description

minutes	Number of minutes until the circuit is switched back to the working interface after the working interface is available.

Command Default

Automatic switchover is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.1CC	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **apsrevert**command to return the circuit to the working interface when it becomes available.

The **apsrevert** command is configured only on protect interfaces.

Examples

The following example shows how to enable circuit 1 on POS interface 5/0/0 to revert to the working interface after the working interface has been available for 3 minutes:

```
Router# configure terminal
Router(config)# interface pos 5/0/0
Router(config-if)# aps protect 1 10.7.7.7
Router(config-if)# aps revert 3
Router(config-if)# end
```

Related Commands

Command	Description
aps protect	Enables a POS interface as a protect interface.

aps timers

To change the time between hello packets and the time before the protect interface process declares a working interface router to be down, use the **apstimers**command in interface configuration mode. To return to the default timers, use the **no** form of this command.

aps timers *seconds1 seconds2*
no aps timers

Syntax Description

seconds1	Number of seconds to wait before sending a hello packet (hello timer). Default is 1.
seconds2	Number of seconds to wait to receive a response from a hello packet before the interface is declared down (hold timer). Default is 3.

Command Default

Hello time is 1 second Hold time is 3 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
11.1CC	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **apstimers**command to control the time between an automatic switchover from the protect interface to the working interface after the working interface becomes available.

Normally, the hold time is greater than or equal to three times the hello time.

The **apstimers** command is configured only on protect interfaces.

Examples

The following example shows how to specify a hello time of 2 seconds and a hold time of 6 seconds on circuit 1 on POS interface 5/0/0:

```
Router# configure terminal
Router(config)# interface pos 5/0/0
Router(config-if)# aps working 1
Router(config-if)# aps timers 2 6
Router(config-if)# end
```

aps unidirectional

To configure a protect interface for unidirectional mode, use the **apsunidirectional** command in controller configuration or interface configuration mode. To return to the default, bidirectional mode, use the **no** form of this command.

aps unidirectional
no aps unidirectional

Syntax Description

This command has no arguments or keywords.

Command Default

Bidirectional mode

Command Modes

Controller configuration Interface configuration

Command History

Release	Modification
11.1CC	This command was introduced.
12.3(11)T	Support for SONET APS using an STM-1 card was added on the Cisco AS5850.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **apsunidirectional**command is configured only on protect interfaces.

Use the **apsunidirectional**command when you must interoperate with SONET network equipment, add/drop multiplexors (ADMs) that supports unidirectional mode.

Note We recommend bidirectional mode when it is supported by the interconnecting SONET equipment. When the protect interface is configured as bidirectional, the working and protect interfaces must cooperate to switch the transmit and receive SONET channel in a bidirectional fashion. This happens automatically when the SONET network equipment is in bidirectional mode.

Examples

The following example shows how to configure POS interface 3/0/0 for unidirectional mode on a Cisco 12000 series router:

```
Router# configure terminal
Router(config)# interface pos 3/0/0
Router(config-if)# aps unidirectional
Router(config-if)# aps protect 1 10.7.7.7
Router(config-if)# end
```

The following example shows how to configure SONET port 0/0 for unidirectional mode on a Cisco AS5850 universal gateway using an STM-1 trunk card:

```
Router# configure terminal
Router(config)# controller sonet 0/0
Router(config-controller)# aps protect
Router(config-controller)# aps unidirectional
Router(config-controller)# end
```

aps working

To configure a Packet over SONET (POS) interface as a working interface, use the **apsworking** command in interface configuration mode. To remove the protect option from the POS interface, use the **no** form of this command.

aps working *circuit-number*
no aps working *circuit-number*

Syntax Description

circuit-number	Circuit number associated with this working interface.

Command Default

No circuit is configured as working.

Command Modes

Interface configuration

Command History

Release	Modification
11.1CC	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When a working interface becomes unavailable because of a router failure, degradation or loss of channel signal, or manual intervention, the circuit is switched to the protect interface to maintain the connection.

To enable the circuit on the protect interface to switch back to the working interface after the working interface becomes available again, use the **apsrevert** command in interface configuration mode.

Caution Configure the working interface before configuring the protect interface to keep the protect interface from becoming the active circuit and disabling the working circuit when it is finally discovered.

Examples

The following example shows how to configure POS interface 0 in slot 4 as a working interface. For information on how to configure the protect interface, refer to the **apsprotect** command.

```
Router# configure terminal
Router(config)# interface pos 4/0/0
Router(config-if)# aps working 1
Router(config-if)# end
```

Related Commands

Command	Description
aps protect	Enables a POS interface as a protect interface.

Command	Description
aps revert	Enables automatic switchover from the protect interface to the working interface after the working interface becomes available.

associate slot

To logically associate slots for automatic protection switching (APS) processor redundancy, use the associate slot command in redundancy configuration mode. To disable slot associations, use the no form of this command.

Single Router APS--Cisco 10000 Series Routers and Cisco uBR10012 Universal Broadband Router
associate slot *slot-one* [*slot-two*]
no associate slot *slot-one* [*slot-two*]

Multirouter APS--Cisco 10000 Series Routers
associate slot *slot-one* **mr-aps**
no associate slot *slot-one* **mr-aps**

Syntax Description

slot-one	**Cisco 10000 Series Router** First slot number to be associated for redundancy. Valid range is from 1 to 8. **Cisco uBR10012 Universal Broadband Router** Specifies the slot that contains the working (primary) card. The available range is 1 to 8, but on the Cisco uBR10012 router the only valid numbers are 1 and 3, and the card must support APS redundancy.
slot-two	**Cisco 10000 Series Router** (Optional) Second slot number to be associated for redundancy. Valid range is from 1 to 8. **Cisco uBR10012 Universal Broadband Router** (Optional) Specifies the slot that contains the redundant (backup) card. The available range is 1 to 8, but on the Cisco uBR10012 router the only valid numbers are 2 and 4. If not specified, the next higher adjacent slot is automatically configured as the redundant slot.
mr-aps	(Cisco 10000 Series Routers Only) Specifies that the slot association is between slots in different routers as part of a multirouter APS configuration.

Command Default

No slots are associated.

Command Modes

Redundancy configuration

Command History

Release	Modification
12.1(5a)EY	This command was introduced.
12.0(23)SX	The mr-aps keyword was added to support multirouter APS on the OC3ATM and OC12ATM line cards for the Cisco 10000 series router.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S, and support was added for the CHOC12, CHSTM1, OC32POS, and OC12POS line cards for the Cisco 10000 series router.
12.2(4)XF1	This command was introduced for the Cisco uBR10012 router.

Release	Modification
12.2(13)BC1	Support was added for the Cisco OC-48 DPT/POS adapter card on the Cisco uBR10012 router.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.

Usage Guidelines

Cisco 10000 Series Router

Use the **associate** command to associate two cards for single-router APS or multirouter APS redundancy protection. Multirouter APS support is specific to the Cisco 10000 series router. Use the mr-aps keyword in a multirouter APS configuration to allow a protect interface on a second router to be a backup for a working interface on the first router.

The associated slots must use the same type of interface module and must support APS redundancy. The cards also must be located in adjacent slots, for example slots 3 and 4.

Cisco uBR10012 Universal Broadband Router

The two cards must be in adjacent slots, with the working card in slot 1 or 3, and the backup card in slot 2 or 4, respectively. The two cards must be identical cards and must support APS redundancy (such as the OC-12 POS line card).

Note You cannot use the **associate** command with any of the Performance Routing Engine (PRE) modules or TCC+ cards, because these cards are automatically configured for redundant operation when two cards are installed in the chassis.

Examples

Single Router APS Example

The following example shows how to associate two slots in the same router in a single router APS configuration:

```
redundancy
 associate slot 3 4
```

Multirouter APS Example on the Cisco 10000 Series Router Only

The following example shows how to associate two separate slots in different routers in a multirouter APS configuration:

```
! Associate slot 3 on first router for APS redundancy
!
redundancy
 associate slot 3 mr-aps
!
! Associate slot 2 on second router for APS redundancy
!
```

```
redundancy
 associate slot 2 mr-aps
```

Related Commands

Command	Description
redundancy	Enters redundancy configuration mode.

association

To configure an association between current node and a remote node, use the **association** command in interprocess communication (IPC) zone configuration mode. To disable this functionality, use the **no** form of this command.

association *association-ID*
no association *association-ID*

Syntax Description

association-ID	Association ID assignment. The value range is from 1 through 255. The association ID must be unique within a specific zone.

Command Default

No association between a current node and a remote node exists.

Command Modes

IPC zone configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

Use the **association** command to configure an association between current node and a remote node. There can be multiple associations within a zone.

Examples

The following example configures an association with an ID of 1:

```
Router(config-ipczone)# association 1
```

Related Commands

Command	Description
ipc zone default	Enters IPC zone configuration mode.
show ipc	Displays IPC statistics.

attach profile-name

To attach alarm profile to port, enter into controller configuration mode, and use the **attach profile-name** command in global configuration mode.

Command to enter into controller configuration mode:

controller **{sonet** | **sdh** | **t1** | **e1** | **t3** | **e3**} *slot*/ /*bay*/*port*
Command to attach alarm profile to port

`attach`*profile-name*

Syntax Description

sonet	Specifies SONET controller
sdh	Specifies SDH controller
t1	Specifies T1 controller
e1	Specifies E1 controller
slot	Specifies the slot number of the interface.
bay	Specifies the bay number of the interface.
port	Specifies the port number of the interface.
profile-name	Alarm profile to attach to the port.

Command Default

None

Command Modes

Configuration mode

Command History

Release	Modification
Cisco IOS XE 16.8.1	Support for this command was introduced on ASR 900 Series.

Usage Guidelines

Enter into the controller configuration mode and then attach the alarm profile to the interface.

Examples

The following example shows how to configure SONET controller in slot 0, bay 3, port 3 and then attach the alarm profile *PORT* to the interface:

```
Router(config)# controller sonet 0/3/3
Router(config-controller)#attach profile PORT
Router(config-controller)#end
```

Related Commands

Command	Description
alarm-profile *name* **chassis** | **card** | **port**}	Creates new alarm profile for chassis, card, or port.

Command	Description
show alarm-profile	Displays alarm profile configured for chassis.

atm sonet

To set the mode of operation and thus control the type of the ATM cell used for cell-rate decoupling on the SONET physical layer interface module (PLIM), use the **atmsonet**command in interface configuration mode. To restore the default Synchronous Transport Signal level 12, concatenated (STS-12c) operation, use the **no** form of this command.

atm sonet [**stm-4**]
no atm sonet [**stm-4**]

Syntax Description

stm-4	(Optional) Synchronous Digital Hierarchy/Synchronous Transport Signal level 4 (SDH/STM-4) operation (ITU-T specification).

Command Default

STS-12c

Command Modes

Interface configuration

Command History

Release	Modification
11.1CC	This command was introduced.
11.2GS	The **stm-4** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use STM-4 in applications in which SDH framing is required.

Use the default (STS-12c) in applications in which the ATM switch requires "unassigned cells" for rate adaptation. An unassigned cell contains 32 zeros.

Examples

The following example shows how to set the mode of operation to SONET STM-4 on ATM interface 3/0:

```
Router(config)#
 interface atm 3/0
Router(config-if)#
 atm sonet stm-4
Router(config-if)#
 end
```

au-3

To configure a particular Administrative Unit type 3 (AU-3) of an E1 line that has been mapped to an AU-3, use the **au-3**command in controller configuration mode.

au-3 *au-3-number*

Syntax Description

au-3-number	Number in the range from 1 to 3.

Command Default

No default behavior or values

Command Modes

Controller configuration

Command History

Release	Modification
12.0(14)S	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
XE Everest 16.6.1	This command was integrated into the Cisco NCS 4200 Series and Cisco ASR 900 Series.

Usage Guidelines

An administrative unit group (AUG) of an STM-1 can be derived from either AU-3s or an AU-4. Use the **augmappingau-3**configuration controller command to map the AUG to an AU-3 with the following muxing/alignment/mapping:

C-12 <--> VC-12 <--> TU-12 <--> TUG-2 <--> VC-3 <--> AU-3 <--> AUG

Configuring the **au-3**command enables you to enter configuration controller au3 command mode and creates a serial interface with the following name format:

slot/port-adapter/port.au-3-number/tug-2-number/e1-number

The aug mapping au-3 and **au-3** commands are available only when Synchronous Digital Hierarchy (SDH) framing is configured.

Examples

The following example shows how to configure AUG mapping to be derived from an AU-3 and selects AU-3 3 to configure as a serial interface:

```
Router(config)# controller sonet 2/0/0
Router(config-controller)# aug mapping au-3
Router(config-ctrlr-au3)# au-3 3
```

Related Commands

Command	Description
au-4 tug-3	Specifies a TUG-3 for configuration.
aug mapping	Configures the AUG mapping mode of the PA-MC-STM-1 to AU-3.

au-4 tug-3

To specify the Administrative Unit type 4 (AU-4) and Tributary Unit group type 3 (TUG-3) number of an E1 line that has been mapped to an AU-4, use the **au-4tug-3**command in controller configuration mode.

au-4 *au-4-number* **tug-3** *tug-3-number*

Syntax Description

au-4-number	Number in the range from 1 to *x*where *x*is the STM level. Default is 1.
tug-3-number	Number in the range from 1 to 3.

Command Default

Default *au-4-number* value for the STM-1 card is 1.

Command Modes

Controller configuration

Command History

Release	Modification
12.0(14)S	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
XE Everest 16.6.1	This command was integrated into the Cisco NCS 4200 Series and Cisco ASR 900 Series.

Usage Guidelines

An AUG of an STM-1 can be derived from either AU-3s or an AU-4. Use the **augmappingau-4**configuration controller command to map the AUG to a TUG-3 with the following muxing/alignment/mapping:

C-12 <--> VC-12 <--> TU-12< --> TUG-2 <--> TUG-3 <--> VC-4 <--> AU-4 <--> AUG

Configuring the **au-4**command enables you to enter configuration controller tug3 command mode and creates a serial interface with the following name format:

slot/port-adapter/port.au-4-number/tug-2-number/e1-number

The aug mapping au-4 and **au-4tug-3**commands are available only when SDH framing is configured.

Examples

The following example shows how to configure AUG mapping to be derived from a TUG-3 and selects TUG-3 1 of AU-4 1:

```
Router(config)# controller sonet 2/0/0
Router(config-controller)# aug mapping au-4
Router(config-ctrlr-tug3)# au-4 1 tug-3 1
```

Related Commands

Command	Description
au-3	Specifies an AU-3 for configuration.
aug mapping	Configures the AUG mapping mode.

aug mapping

To configure administrative unit group (AUG) mapping when Synchronous Digital Hierarchy (SDH) framing is selected, use the **augmapping** command in controller configuration mode.

aug mapping {**au-3** | **au-4**}

Syntax Description

au-3	Specifies use of three paths--a path is known as an Administrative Unit (AU)--consisting of seven Tributary Unit group type 2s (TUG-2s). Each TUG-2 consists of three virtual containers (VC-12s), which carry E1 lines resulting in 21 E1 lines within one AU-3 path.
au-4	Specifies use of one path consisting of three TUG-3 types. Each TUG-3 consists of seven TUG-2s, resulting in a total of 63 E1 lines within one AU-4 path. This is the default.

Command Default

au-4

Command Modes

Controller configuration

Command History

Release	Modification
12.0(14)S	This command was introduced.
12.0(17)S	Support for the two-port STM-1/OC-3 channelized E1/T1 line card was added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
XE Everest 16.6.1	This command was integrated into the Cisco NCS 4200 Series and Cisco ASR 900 Series.

Usage Guidelines

In SDH, there are two possible mapping/multiplexing schemes for most payload types: ANSI and ETSI.

In ANSI mapping, the Low Order payloads are aggregated into a VC-3 High Order Path. An AU pointer is added to the VC-3 to create an AU-3. Three such AU-3s are then synchronously multiplexed into an AUG. The multiplexing scheme is as follows:

... VC-3 <-> AU-3 (x3) <-> AUG <-> STM-1

SDH ANSI mapping is very similar to the SONET frame structure.

In ETSI mapping, the Low Order payloads are aggregated into a VC-4 High Order Path. An AU pointer is added to the VC-4 to create an AU-4 (Administrative Unit type 4). One AU-4 is "multiplexed" into an AUG (AU group), which is to say, the AUG is, in fact, equivalent to an AU-4. The multiplexing scheme is as follows:

... TUG-3 (x3) <-> VC-4 <-> AU-4 (x1) <-> STM-1

This command is available only when SDH framing is configured.

This command does not have a **no** form because data must flow using one of the two mapping/multiplexing schemes.

Examples

The following example shows how to configure AU-3 mapping for the STM-1 trunk card:

```
Router(config)# controller sonet 1/0
Router(config-controller)# aug mapping au-3
```

aug mapping [au-3 | au-4] stm [stm number] stm1 number [number]

Use this command to configure mixed AU-3 and AU-4 mapping

aug mapping [*au-3* | *au-4*] **stm** [*stm number*] **stm1 number** [*number*].

Syntax Description

Syntax Description

au-3	Mode of augment mapping
au-4	Mode of augment mapping
stm	The STM-1 (Synchronous Transport Module level-1) is the SDH ITU-T fiber optic network transmission standard. It has a bit rate of 155.52 Mbit/s.
stm1 number	The STM number ranges from 1 to 4.

Command Default

The default mode is AU-4.

Command Modes

Global configuration

Command History

Release	Modification
XE Everest 16.6.1	This command was integrated into the Cisco NCS 4200 Series and Cisco ASR 900 Series.

Usage Guidelines

The **aug mapping** command is available only when SDH framing is configured. AUG mapping is supported at STM-1 level.

Examples

```
enable
configure terminal
aug mapping [au-3 | au-4 stm [1-1] stm1 number [1-4]
end
```

Related Commands

Command	Description
show running configuration	Verifies aug mapping configuration.

aug mapping au-3 stm [stm number] path number [path number]

Use this command to change the AUG mapping of a particular STM-1 to AU-3.

aug mapping *au-3* **stm** [*1-16*] **path number** [*1-16*].

Syntax Description

Syntax Description

au-3	Mode of augment mapping
au-4	Mode of augment mapping
stm	The STM-1 (Synchronous Transport Module level-1) is the SDH ITU-T fiber optic network transmission standard. It has a bit rate of 155.52 Mbit/s.
path number	The path parameter number ranges from 1 to 16.

Command Default

The default mode is AU-4.

Command Modes

Global configuration

Command History

Release	Modification
XE Everest 16.6.1	This command was integrated into the Cisco NCS 4200 Series and Cisco ASR 900 Series.

Examples

```
enable
configure terminal
aug mapping [au-3 | au-4 stm [1-16] path number [1-16]
end
```

Related Commands

Command	Description
show running configuration	Verifies aug mapping configuration.

auto-polarity

To enable automatic receiver polarity reversal on a hub port connected to an Ethernet interface of a Cisco 2505 or Cisco 2507 router, use the **auto-polarity** command in hub configuration mode. To disable this function, use the **no** form of this command.

auto-polarity
no auto-polarity

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Hub configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command applies to a port on an Ethernet hub only.

Examples

The following example shows how to enable automatic receiver polarity reversal on hub 0, ports 1 through 3:

```
Router(config)#
 hub ethernet 0 1 3
Router(config-hub)#
 auto-polarity
```

Related Commands

Command	Description
hub	Enables and configures a port on an Ethernet hub of a Cisco 2505 or Cisco 2507 router.

b2 sd-ber

To set the signal degrade bit-error rate (BER) threshold values, use the **b2sd-ber**command in controller configuration mode. To return to the default setting, use the **no** form of this command.

b2 sd-ber *rate*
no b2 sd-ber

Syntax Description

rate	Bit-error rate from 3 to 9 (10-n). The value of 9 represents better quality, and the value of 3 represents lower quality. The default is 6.

Command Default

rate: 6

Command Modes

Controller configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to configure the threshold for degradation of quality of signal with b2 errors.

Examples

The following example shows how to configure a signal degrade BER threshold value of 7 on the SONET controller:

```
Router(config)# controller sonet 1/0
Router(config-controller)# b2 sd-ber 7
```

Related Commands

Command	Description
show controllers sonet	Displays information about the SONET controllers.

b2 sf-ber

To set the signal failure bit-error rate (BER) threshold values, use the **b2sf-ber**command in controller configuration mode. To return to the default setting, use the **no** form of this command.

b2 sf-ber *rate*
no b2 sf-ber *rate*

Syntax Description

rate	Bit-error rate from 3 to 9 (10-n). The value of 9 represents better quality, and the value of 3 represents lower quality. The default is 3.

Command Default

rate : 3

Command Modes

Controller configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Use this command to configure the threshold for failure of quality of signal with b2 errors. The value of 9 represents better quality and the value of 3 represents lower quality.

Examples

The following example shows how to configure a signal failure BER threshold value of 7 on the SONET controller:

```
Router(config)# controller sonet 1/0
Router(config-controller)# b2 sf-ber 7
```

Related Commands

Command	Description
show controllers sonet	Displays information about the SONET controllers.

backup delay

To define how much time should elapse before a secondary line status changes after a primary line status has changed, use the **backupdelay**command in interface configuration mode. To return to the default so that as soon as the primary fails, the secondary is immediately brought up without delay, use the **no** form of this command.

backup delay {*enable-delay-period* | **never**} {*disable-delay-period* | **never**}
no backup delay {*enable-delay-period* | **never**} {*disable-delay-period* | **never**}

Syntax Description

enable-delay-period	Number of seconds that elapse after the primary line goes down before the Cisco IOS software activates the secondary line.
disable-delay-period	Number of seconds that elapse after the primary line comes up before the Cisco IOS software deactivates the secondary line.
never	Secondary line is never activated or deactivated.

Command Default

0 second delay

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.2(33)SRB1.
15.1(2)SNH	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

For environments in which spurious signal disruptions appear as intermittent lost carrier signals, we recommend that you enable some delay before activating and deactivating a secondary line.

For the Cisco 7600 Backup Interface for Flexible UNI feature to work correctly, the enable and disable backup delay must be 0.

Examples

The following example sets a 10-second delay on deactivating the secondary line (serial interface 0); however, the line is activated immediately.

```
interface serial 0
 backup delay 0 10
```

backup interface

To configure an interface as a secondary or a dial backup, use the **backupinterface**command in interface configuration mode. To disable the interface from serving as a backup, use the **no** form of this command.

Cisco 7200 Series and Cisco 7600 Series Routers Only

backup interface *slot / port-adapter / port*

no backup interface *slot / port-adapter / port*

Other Cisco Routers

backup interface *type number*

no backup interface *type number*

Syntax Description

slot / port-adapter / port	Chassis slot, port adapter, and port number of the interface to configure as a backup. Include a slash (/) between the slot, port adapter, and port (for example, 1/1/1). See your hardware installation manual for the specific slot, port adapter, and port numbers.
type number	Type and port number of the interface that is being configured as a backup.

Command Default

An interface is not configured as a backup.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.2(33)SRB1.

Usage Guidelines

The interface that you define with the **backupinterface** command can back up only one interface.

Serial, ISDN, and Ethernet backup interfaces are supported by the routers. Access servers support both asynchronous backup interfaces and serial backup interfaces.

In Cisco IOS Release 12.2(33)SRB1 and later releases, you can configure a backup interface for Gigabit Ethernet interface on the Cisco 7600 router. The backup interface works only when the configurations on the primary and backup interfaces are identical. This is applicable to all Cisco IOS platforms and interfaces.

Note If the interface configuration includes the **xconnect**command, you must specify a different virtual circuit ID (VCID) on the primary and backup interfaces.

Examples

The following example sets serial interface 1 as the backup line to serial interface 0:

```
Router(config)# interface serial 0
Router(config-if)# backup interface serial 1
```

The following example sets Gigabit Ethernet interface 4/0/1 as the backup interface for Gigabit Ethernet interface 3/0/1 on the Cisco 7600 router:

```
Router(config)# interface gigabitEthernet 3/0/1
Router(config-if)# backup interface gigabitEthernet 4/0/1
```

Related Commands

Command	Description
aps protect (SONET)	Enables SONET APS.
show version	Displays information about the currently loaded software along with hardware and device information.

backup interface atm

To back up a locally switched ATM connection, use the **backupinterfaceatm**command in **theconnectsub**mode. To deconfigure the active routing policy set, leaving the SBE with no active routing policy set, use the **no** form of this command.

backup interface atm *x/y/z vpi/vci*
no backup interface atm *x/y/z vpi/vci*

Syntax Description

interface	Identifies the interface.
atm > *x* / *y* / *z* >	Specifies the backup location for the ATM slot/subslot/port to be backed up.
vpi / *vci* >	Specifies the backup location for the ATM virtual path identifier/virtual channel identifier (VPI/VCI).

Command Default

No default behavior or values.

Command Modes

Connect submode (config-connection)

Command History

Release	Modification
12.2(33)SRC	This command was introduced on the Cisco 7600 series routers.

Usage Guidelines

- Only the tail end AC can be backed up; if head end fails there is no protection.
- The circuit type of the primary and backup AC must be identical (failover operation will not switch between different types of interfaces).
- Autoconfiguration is allowed for backup ATM Permanent Virtual Circuits (PVCs) or ATM Permanent Virtual Paths (PVPs).
- Dynamic modification of parameters in a local switching connection is not supported in the case where the tail-end segment is backed up to a segment using the **backupinterfaceatm**command. If you want to modify the parameters in any of the three segments (head-end, tail-end, or backup segment), you must first unconfigure with the **backupinterfaceatm** command, make the changes in the individual segments, and then reconfigure the backup with the **backupinterfaceatm** command.

Examples

The following is an example of a ATM virtual path local switching backup:

```
Router(config)# connect ATM atm2/0/0 0 atm3/0/0 0
Router(config-connection)# backup interface atm 4/0/0 1
```

The following is an example of a ATM virtual channel local switching backup:

```
Router(config)# connect ATM atm2/0/0 24/56 atm3/0/0 24/57
Router(config-connection)# backup interface atm 4/0/0 25/58
!
```

Related Commands

Command	Description
connect atm	Configures a local switching connection.

backup interface cem

To back up a locally switched CEM connection, use the **backupinterfacecem** command in **theconnectsub**mode. To deconfigure the locally switched CEM connection backup, use the **no** form of this command.

backup interface cem *x/y/z cemckt*
no backup interface cem *x/y/z cemckt*

Syntax Description

interface >	Identifies the interface.
cem > *x* / *y* / *z*	Specifies the CEM interface slot, subslot, and port to be backed up.
cemckt	Specifies the backup location for the CEM.

Command Default

No default behavior or values.

Command Modes

Connect submode (config-connection)

Command History

Release	Modification
12.2(33)SRC	This command was introduced on the Cisco 7600 series routers.

Usage Guidelines

- Autoconfiguration of CEM interfaces is not supported.
- Only the tail end AC can be backed up; if head end fails there is no protection.
- The circuit type of the primary and backup AC must be identical (failover operation will not switch between different types of interfaces or different CEM circuit types).
- Backs up a local switching connection to cem-ckt3 of CEM interface cem3. Only one backup AC is allowed for each connection.
- Autoconfiguration of backup CEM circuits is not allowed.
- The CEM circuit used as a backup in a local switching connection cannot be used for xconnect configurations.
- Dynamic modification of parameters in a local switching connection is not supported in the case where the tail-end segment is backed up to a segment using the **backupinterfacecem**command. If you want to modify the parameters in any of the three segments (head-end, tail-end, or backup segment), you must first unconfigure with the **backupinterfacecem**command, make the changes in the individual segments, and then reconfigure the backup with the **backupinterfacecem** command.

Examples

The following is an example of a CEM local switching backup:

```
Router(config)# connect cema cem4/3/0 0 cem2/0/0 0
Router(config-connection)# backup interface cem 2/0/0 1
```

Related Commands

Command	Description
connect cem	Configures a local switching connection.

backup load

To set a traffic load threshold for dial backup service, use the **backupload**command in interface configuration mode. To return to the default value, use the **no** form of this command.

backup load {*enable-threshold* | **never**} {*disable-load* | **never**}
no backup load {*enable-threshold* | **never**} {*disable-load* | **never**}

Syntax Description

enable-threshold	Percentage of the primary line's available bandwidth that the traffic load must exceed to enable dial backup.
disable-load	Percentage of the available bandwidth that the traffic load must be less than to disable dial backup. The transmitted or received load on the primary line plus the transmitted or received load on the secondary line is less than the value entered for the *disable-load*argument to disable dial backup.
never	The secondary line is never activated or deactivated because of the traffic load.

Command Default

No threshold is defined.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.2(33)SRB1.

Usage Guidelines

When the transmitted or received load on the primary line is greater than the value assigned to the *enable-threshold* argument, the secondary line is enabled.

The secondary line is disabled when one of the following conditions occurs:

- The transmitted load on the primary line plus the transmitted load on the secondary line is less than the value entered for the *disable-load*argument.
- The received load on the primary line plus the received load on the secondary line is less than the value entered for the *disable-load* argument.

If the **never**keyword is used instead of an *enable-threshold*argument, the secondary line is never activated because of traffic load. If the **never** keyword is used instead of a *disable-load* argument, the secondary line is never activated because of traffic load.

Examples

The following example sets the traffic load threshold to 60 percent of the primary line serial 0. When that load is exceeded, the secondary line is activated and will not be deactivated until the combined load is less than 5 percent of the primary bandwidth.

```
interface serial 0
 backup load 60 5
 backup interface serial 1
```

bandwidth (interface configuration)

To set the inherited and received bandwidth values for an interface, use the **bandwidth** command in interface or virtual network interface config mode. To restore the default values, use the **no** form of this command.

bandwidth [{**receive**}] {*kbps* | **inherit** [{*kbps*}]}
no bandwidth [{**receive**}] {*kbps* | **inherit** [{*kbps*}]}

Syntax Description

kbps	Intended bandwidth, in kilobits per second. The range is from 1 to 10000000. For a full bandwidth DS3 line, enter the value 44736.
inherit	(Optional) Specifies how a subinterface inherits the bandwidth of its main interface.
receive	(Optional) Enables asymmetric transmit/receive operations so that the transmitted (**inherit** *kbps*) and received bandwidth are different.

Command Default

Default bandwidth values are set during startup. The bandwidth values can be displayed using the **show interfaces** or **show ipv6 interface** command. If the **receive** keyword is not used, by default, the transmit and receive bandwidths will be assigned the same value.

Command Modes

Interface configuration (config-if)

Virtual network interface (config-if-vnet)

Command History

Release	Modification
10.0	This command was introduced.
12.2T	This command was modified. The **inherit** keyword was added.
12.4(6)T	This command was modified. Support for IPv6 was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 Aggregation Services Series Routers.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.
15.1(03)S	This command was modified. Support was added for the **receive** keyword.

Usage Guidelines

Bandwidth Information

The **bandwidth** command sets an informational parameter to communicate only the current bandwidth to the higher-level protocols; you cannot adjust the actual bandwidth of an interface using this command.

Note This is only a routing parameter. It does not affect the physical interface.

Changing Bandwidth

For some media, such as Ethernet, the bandwidth is fixed; for other media, such as serial lines, you can change the actual bandwidth by adjusting the hardware. For both classes of media, you can use the **bandwidth** command to communicate the current bandwidth to the higher-level protocols.

Bandwidth Inheritance

Before the introduction of the **bandwidth inherit** command option, when the bandwidth value was changed on the main interface, the existing subinterfaces did not inherit the bandwidth value. If the subinterface was created before the bandwidth was changed on the main interface, the subinterface would receive the default bandwidth of the main interface, and not the configured bandwidth. Additionally, if the router was subsequently reloaded, the bandwidth of the subinterface would then change to the bandwidth configured on the main interface.

The **bandwidth inherit** command controls how a subinterface inherits the bandwidth of its main interface. This functionality eliminates inconsistencies related to whether the router has been reloaded and what the order was in entering the commands.

The **no bandwidth inherit** command enables all subinterfaces to inherit the default bandwidth of the main interface, regardless of the configured bandwidth. If the **bandwidth inherit** command is used without configuring a bandwidth on a subinterface, all subinterfaces will inherit the current bandwidth of the main interface. If you configure a new bandwidth on the main interface, all subinterfaces will use this new value.

If you do not configure a bandwidth on the subinterface and you configure the **bandwidth inherit** *kbps* command on the main interface, the subinterfaces will inherit the specified bandwidth.

In all cases, if an explicit bandwidth setting is configured on an interface, the interface will use that setting, regardless of whether the bandwidth inheritance setting is in effect.

Bandwidth Receipt

Some interfaces (such as Asymmetric Digital Subscriber Line (ADSL), V.35, RS-449, and High-Speed Serial Interface (HSSI)) can operate with different transmit and receive bandwidths. The **bandwidth receive** command permits this type of asymmetric operation. For example, for ADSL, the lower layer detects the two bandwidth values and configures the Integrated Data Base (IDB) accordingly. Other interface drivers, particularly serial interface cards on low- and midrange-platforms, can operate in this asymmetric bandwidth mode but cannot measure their clock rates. In these cases, administrative configuration is necessary for asymmetric operations.

Examples

The following example shows how to set the full bandwidth for DS3 transmissions:

```
Router(config)# interface serial 0
Router(config-if)# bandwidth 44736
```

The following example shows how to set the receive bandwidth:

```
Router(config)# interface serial 0
Router(config-if)# bandwidth receive 1000
```

Related Commands

Command	Description
show interfaces	Displays statistics for all interfaces configured on the router.
show ipv6 interface	Displays statistics for all interfaces configured on the IPv6 router.

batch

To allow better cache utilization at the interface level, use the batch command under interface configuration mode.

batch {allowed | **count***number* | **threshold***range* **}**

Syntax Description

allowed	Enables the batch process for packets received.
count *number*	Number of interrupts received for the batch process. Value ranges from 2 to 8. When batching is enabled, the packets in the receive ring are processed on every nth RX interrupt, where "n" is configured by "batch count n".
threshold *range*	Packets per 4ms threshold to enable the batch. Range is from 2 to 100 packets/4ms. If the number of packets received within a 4ms period exceeds 'x' then batching is turned on, otherwise it is turned off.

Command Default

Batch is disabled.

Command Modes

configuration-Interface

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

Use this command to increase the performance of packets processing through the interface to optimize the cache usage. The performance improvement varies depending on the burstiness of the traffic. The traffic with high burstiness provides better performance.

The **batch** command is disabled by default. The batch process depends on the batch threshold (x) which is the number of packets received within a ‘y’ ms period. The batch process is turned on if the number of packets received within a ‘y’ ms period exceeds ‘x’, otherwise it is turned off.

Currently, the batch command is supported at the interface level on Cisco 890 routers only.

Examples

The following example shows the batch command configured in interface fastethernet ports:

```
        !
!
interface FastEthernet0
 no ip address
 batch allowed
 batch count 6
 batch threshold 75
!
interface FastEthernet1
 no ip address
 batch allowed
 batch count 6
 batch threshold 75
!
```

```
interface FastEthernet2
 no ip address
 batch allowed
 batch count 6
 batch threshold 75
!
interface FastEthernet3
 no ip address
 batch allowed
 batch count 6
 batch threshold 75
!
interface FastEthernet4
 no ip address
 batch allowed
 batch count 6
 batch threshold 75
!
interface FastEthernet5
 no ip address
 batch allowed
 batch count 6
 batch threshold 75
!
interface FastEthernet6
 no ip address
 batch allowed
 batch count 6
 batch threshold 75
!
interface FastEthernet7
 no ip address
 batch allowed
 batch count 6
 batch threshold 75
!
!
```

bert abort controller

To end a bit error rate testing (BERT) session, use the **bertabortcontroller**command in privileged EXEC mode.

bert abort controller *controller-type slot*/*port*

Syntax Description

controller-type	Type of controller being tested. Use either T1 or E1 depending on the type of facility.
slot / *port*	Slot number and port number to end a BERT session.

Command Default

A BERT session is configured.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(2)XD	This command was introduced.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **bertabortcontroller**command to cancel bit error rate testing on each port of the Cisco AS5300 router.

The BERT feature enables you to test the quality of the connected Primary Rate Interface (PRI) links by direct comparison of a pseudorandom or repetitive test pattern with an identical locally generated test pattern.

Examples

The following is sample output from the **bertabortcontroller**command when no bit error rate test is running:

```
Router# bert abort controller t1 0/0
Router#
17:53:33: There is no BERT Test running ....
```

The following is sample output from the **bertabortcontroller**command when a bit error rate test is running:

```
Router# bert abort controller t1 0/0
Do you really want to abort the current BERT [confirm] Y17:56:56: %BERT-6-BERT_RESULTS:
Controller T1 0 Profile default : The Test was
aborted by User
```

Related Commands

Command	Description
bert controller	Starts a bit error rate test for a particular port.

Command	Description
bert pattern (**T1/E1**)	Sets up various bit error rate testing profiles.

bert controller

To start a bit error rate test (BERT) for a particular port, use the **bertcontroller**command in privileged EXEC mode.

bert controller *controller-type controller-number last-controller-number* **profile** {*profile-number* [*last-profile-number*] [**timeslot** *timeslot-number* [*last-timeslot-number*]] | **default**}

Syntax for Cisco 2600 Platforms

bert controller *type-controller slot/port* [**channel-group** *channel-number*] [**pattern** *pattern-name*] [**interval** *range*]

Syntax Description

controller-type	Type of controller being tested. Use either T1 or E1 depending on the type of facility.
controller-number	Controller number. The valid range is from 0 to 7.
last-controller-number	Last contoller number. The valid range is from 2 to 7.
profile	Sets the profile numbers for the bit error rate test.
profile-number	Numbers of the test profiles to use. The valid range is from 0 to 15. The default is 0.
last-profile-number	(Optional) Last profile number. The default is 0.
timeslot	(Optional) Generates the data based on the timeslots associated with the controller.
timeslot-number	(Optional) Timeslot number. The valid range is from 1 to 22.
last-timeslot-number	(Optional) Last timeslot number. The valid range is from 1 to 24.
default	Executes the default bit error rate test (0).
slot/port	Slot and port number for the ports to be tested.
channel-group *channel-number*	(Optional) Specifies the channel group number that you want the BERT test to run on. Numbers can be 0 or 1.

pattern *pattern-name*	(Optional) BERT patterns available for testing are: • 0s--repetitive pattern; all zeros test pattern • 1s--n repetitive pattern; all ones test pattern • qrw--215-1 QRW test pattern • qrss (default)--220-1 Quasi-Random Signal Sample 0.151 test pattern • alt-0-1--alternating zeros and ones test pattern • 1in8--n repetitive pattern; 1 in 8 • 3in24--n repetitive pattern; 3 in 24 • 63--26-1 63 test pattern • 511--29-1 511 test pattern • 2047--211-1 test pattern
interval *range*	(Optional) Range for the test, in minutes. The valid range is from 1 to 14400. The default is 1.

Command Default

The test profile 0 is configured by default.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(2)XD	This command was introduced.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The following keywords and arguments were added: • *last-controller-number* • *last-profile-number* • **timeslot** • *timeslot-number* • *last-timeslot-number* • **default**

Usage Guidelines

Use the **bertcontroller** command to start a bit error rate test for a particular port on a Cisco AS5300 router.

Quality Testing

The BERT feature enables you to test the quality of the connected Primary Rate Interface (PRI) links by direct comparison of a pseudorandom or repetitive test pattern with an identical locally generated test pattern.

E1 Controllers

The E1 controller cannot be set in loopback mode from the Cisco AS5300 router. For the **bertcontroller** command to work correctly with the E1 controller, the controller must be configured as a channel group or as channel-associated signaling (CAS) and the line must be configured as a remote loop from the switch side of the link.

You can use the **channel-group***channel-group-number* keyword and argument combination to specify a channel-group. If the channel-group is specified, BERT will be run on the timeslots associated with the channel group only. Otherwise, BERT will run on all the timeslots of the specified controller.

Examples

The following is sample output from the **bertcontroller** command:

```
Router#
bert controller T1 T2 profile default
Press <Return> to start the BERT [confirm]
Y
17:55:34: %BERT-6-BERT_START: Starting BERT on Interface 0 with Profile default
Data in current interval (10 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
```

Table 1 describes the significant fields shown in the display.

*Table 1: **bert controller** Field Descriptions*

Field	Description
Data in current interval	Shows the current accumulation period, which rolls into the 24-hour accumulation every 15 minutes. As the latest 15-minute accumulation period enters the buffer, the oldest 15-minute period is deleted. The accumulation period is from 1 to 900 seconds.
Line Code Violations	For alternate mark inversion (AMI)-coded signals, a line code violation is a bipolar violation (BPV) occurrence. Indicates the occurrence of either a BPV or an excessive zeros (EXZ) error event.
Path Code Violations	When super frame (SF) (D4) framing is used, a path code violation is a framing error. When extended super frame (ESF) framing is used, a path code violation is a cyclic redundancy check type 6 (CRC-6) error. Indicates a frame-synchronization bit error in the D4 and E1-non-CRC formats, or a CRC error in the ESF and E1-CRC formats.
Slip Secs	Indicates the replication or deletion of the payload bits of a DS1 frame. A slip may be indicated when there is a difference between the timing of a synchronous receiving terminal and the received signal.
Fr Loss Secs	Seconds during which the framing pattern has been lost. Indicates the number of seconds for which an Out-of-Frame error is detected.

Field	Description
Line Err Secs	A line error second (LES) is a second in which one or more line code violation (LCV or CV-L) errors are detected.
Degraded Mins	A degraded minute is one in which the estimated error rate exceeds 1-6 but does not exceed 1-3.
Errored Secs	In extended superframe (ESF) and E1-CRC links, an errored second is a second in which one of the following is detected: one or more path code violations; one or more Out-of-Frame defects; one or more controlled slip events; an alarm indication signal (AIS) defect. For D4 and E1-non-CRC links, the presence of bipolar violations also triggers an errored second.
Bursty Err Secs	Seconds with fewer than 320 and more than 1 path code violation error, no severely errored frame defects, and no detected incoming AIS defects. Controlled slips are not included in this parameter.
Severely Err Secs	For ESF signals, a second with one of the following errors: 320 or more path code violation errors; one or more Out-of-Frame defects; a detected AIS defect. For E1-CRC signals, a second with one of the following errors: 832 or more path code violation errors; one or more Out-of-Frame defects. For E1-non-CRC signals, a second with 2048 or more line code violations. For D4 signals, a count of 1-second intervals with framing errors, or an Out-of-Frame defect, or 1544 line code violations.
Unavail Secs	Count for every second in which an unavailable signal state occurs. This term is used by new standards in place of failed seconds (FS).

The following example shows a BERT test started on a T1 port 0/0 and channel group 0 with a QRSS signaling pattern for a duration of 5 minutes:

```
Router# bert controller t1 0/0 channel-group 0 pattern qrss interval 5
```

Related Commands

Command	Description
bert abort	Aborts a bit error rate testing session.
bert pattern (T1/E1)	Sets up various bit error rate testing profiles.
bert abort controller	Stops a BERT test prematurely.

bert errors

To transmit bit error ratio test (BERT) errors while running any BERT pattern, use the**berterror**command in interface configuration mode.

bert errors [*number*]

Syntax Description

number	(Optional) Range of **1-255**BERT errors that may be introduced in a BERT pattern.

Command Default

Default is 1.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(12c)EX1	This command was introduced for Cisco 7304 routers.
12.2(18)S	This command was introduced on Cisco 7304 routers running Cisco IOS Release 12.2S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE to support SPAs on the Cisco 7600 series router and Catalyst 6500 series switch.
12.2(25)S3	This command was integrated into Cisco IOS Release 12.2(25)S3.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command to test link availability by injecting a fixed number of bert errors when a pattern is running and check that the same number of errors were received on the remote end.

Examples

This example injects 200 BERT errors in a running bit pattern on slot 5, subslot 0.

```
Router# configure terminal
Router(config)# interface serial 5/0/0
Router(config-if)# bert errors 200
```

Related Commands

Command	Description
bert pattern	Starts a BERT pattern on a port.
show controller serial	Displays serial line statistics.

bert pattern

To start a BERT pattern on a port, use the **bertpattern**command in interface configuration mode. Use the no bert pattern command to stop the sequence.

bert pattern {**0s** | **1s** | **2^11** | **2^15** | **2^20** | **2^23** | **alt-0-1** | **qrss**} **interval** *minutes*
no bert pattern {**0s** | **1s** | **2^11** | **2^15** | **2^20** | **2^23** | **alt-0-1** | **qrss**} **interval** *minutes*

Syntax Description

0s	Repeating pattern of zeros (...000...).
1s	Repeating pattern of ones (...111...).
2^11	Pseudo-random repeating test pattern that consists of 2,048 bits.
2^15	Pseudorandom 0.151 test pattern that is 32,768 bits in length.
2^20	Pseudorandom 0.153 test pattern that is 1,048,575 bits in length.
2^23	Pseudorandom 0.151 test pattern that is 8,388,607 bits in length.
alt-0-1	Repeating pattern of alternating zeros and ones (...01010...).
qrss	Pseudorandom quasi-random signal sequence (QRSS) 0.151 test pattern that is 1,048,575 bits in length.
interval *minutes*	Specifies the length of the BERT test in minutes.

Command Default

Bert is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
11.1CC	The command was introduced.
12.0(5)XE	The command was enhanced as an ATM interface configuration command
12.0(7)XE1	Support for Cisco 7100 series routers was added.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.1(12c)EX1	Support for Cisco 7304 routers was added.
12.2(18)S	Support for Cisco 7304 routers was added.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE to support SPAs on the Cisco 7600 series router and the Catalyst 6500 series switch.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.2(25)S3	This command was integrated into Cisco IOS Release 12.2(25)S3.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
XE3.18SP	This command was integrated into Cisco NCS 4200 Series.
XE Everest 16.5.1	This command was implemented on the Cisco ASR 920 Routers and Cisco NCS 4200 Series.

Usage Guidelines

Use the bert pattern commamd to start or stop a specific bit pattern. To test link availability, start a pattern on one end and put the remote end in network loopback and verify that there are no bert errors.

Examples

This example starts a bert pattern on slot 5, bay 0.

```
Router# configure terminal
Router(config)# int serial 5/0/0
Router(config-if)# bert pattern 0s
```

This example starts a bert pattern pRBS.

```
Router#enable
Router#configure terminal
Router(config)#bert pattern pRBS interval 5 direction line
exit
```

Related Commands

Command	Description
bert errors	Transmit bert errors while running any bert pattern.
loopback	Loopback at various points in the transmit and receive path.
show controller serial	Displays serial line statistics.
show controller sonet	Displays sonet interface module statistics.
show controller t1	Displays t1 interface module statistics.
show controller t3	Displays t3 interface module statistics.

bert pattern (T1 E1)

To enable a bit error rate test (BERT) pattern on a T1 or E1 line, use the**bertpattern**command in controller configuration mode. To disable a BER test pattern, use the **no** form of this command.

bert pattern *pattern* **interval** *time*
no bert pattern *pattern* **interval** *time*

Syntax Description

pattern	The test pattern indicated by any of the following allowable values:
2^23	Invokes a pseudorandom 0.151 test pattern that is 8,388,607 bits in length.
2^20	Invokes a pseudorandom 0.153 test pattern that is 1,048,575 bits in length.
2^20-QRSS	Invokes a pseudorandom quasi-random signal sequence (QRSS) 0.153 test pattern that is 1,048,575 bits in length.
2^15	Invokes a pseudorandom 0.151 test pattern that is 32,768 bits in length.
2^11	Invokes a pseudorandom test pattern that is 2,048 bits in length.
1s	Invokes a repeating pattern of ones (...111...).
0s	Invokes a repeating pattern of zeros (...000...).
alt-0-1	Invokes a repeating pattern of alternating zeros and ones (...01010...).
interval *time*	Specifies the duration (in minutes) of the BER test. The interval can be a value from 1 to 14400. There is no default.

Command Default

Disabled

Command Modes

Controller configuration

Command History

Release	Modification
11.1CC	This command was introduced.
12.0(5)XE	This command was enhanced as an ATM interface configuration command.
12.0(7)XE1	This command was implemented on Cisco 7100 series routers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

BER testing is supported on each of the T1 or E1 lines, is done only over an unframed T1 or E1 signal, and is run on only one port at a time.

To view the BER test results, use the **showcontrollersatm**EXEC command. The BERT results include the following information:

- Type of test pattern selected
- Status of the test
- Interval selected
- Time remaining on the BER test
- Total bit errors
- Total bits received

When the T1 or E1 line has a BER test running, the line state is DOWN and the status field shows the current/last result of the test.

The**bertpattern**command is not written to NVRAM because this command is only used to test the T1 or E1 line for a short predefined interval, and to avoid accidentally saving the command.

Examples

The following example shows how to run a BERT pattern of all zeros on a Cisco 7200 series router for 30 minutes on the T1 controller in slot 1:

```
Router(config)#
controller T1 1/0
Router(config-if)#
bert pattern 0s interval 30
```

Related Commands

Command	Description
show controllers atm	Displays information about T1/E1 links in Cisco 7100 series routers, Cisco 7200 series routers, and Cisco 7500 series routers.

bert pattern (T3 E3)

To enable a bit error rate test (BERT) pattern on a T3 or E3 controller, use the **bertpattern** command in controller configuration mode. To disable a BER test pattern, use the no form of this command.

bert pattern *pattern* **interval** *time*
no bert pattern

Syntax Description

pattern	The pattern indicated by any of the following allowable values:
2^23	Invokes a pseudorandom 0.151 test pattern that is 8,388,607 bits in length.
2^20	Invokes a pseudorandom 0.153 test pattern that is 1,048,575 bits in length.
2^15	Invokes a pseudorandom 0.151 test pattern that is 32,768 bits in length.
1s	Invokes a repeating pattern of ones (...111...).
0s	Invokes a repeating pattern of zeros (...000...).
alt-0-1	Invokes a repeating pattern of alternating zeros and ones (...01010...).
interval *time*	Specifies the duration (in minutes) of the BER test. The interval can be a value from 1 to 14400. There is no default.

Command Default

Disabled

Command Modes

Controller configuration

Command History

Release	Modification
11.1CC	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(11)YT	This command was integrated into Cisco IOS Release 12.2(11)YT and implemented on the following platforms: Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3660 series, Cisco 3725, and Cisco 3745 routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

BER testing is supported on T3/E3 links and is done only over framed T3 or E3 signals, unless E3 framing is in bypass mode.

To display the BER test results, use the show controllers t3 or show controllers e3 EXEC command. The BER test results include the following information:

- Type of test pattern selected
- Status of the test
- Interval selected
- Time remaining on the BER test
- Total bit errors
- Total bits received

When the T3 or E3 line has a BER test running, the line state is DOWN and the status field shows the current or last result of the test.

The**bertpattern**command is not written to NVRAM because this command is used only to test the T3 or E3 line for a short predefined interval, and to avoid accidentally saving the command.

Examples

The following example shows how to run a BERT pattern of all zeros for 30 minutes on the T3 controller in slot 1:

```
Router(config)#
controller T3 1/0
Router(config-if)#
bert pattern 0s interval 30
```

Related Commands

Command	Description
show controllers e3	Displays information about E3 controllers.
show controllers t3	Displays information about T3 controllers.

bert profile

To set up various bit error rate testing profiles, use the **bert profile** command in global configuration mode. To disable the particular bit error rate test (BERT) profile indicated by profile number, use the **no** form of this command.

bert profile *number* **pattern** *pattern* **threshold** *threshold* **error-injection** *err-inj* **duration** *time*
no bert profile *number* **pattern** *pattern* **threshold** *threshold* **error-injection** *err-inj* **duration** *time*

Syntax Description

number	BERT profile number. The valid range is from 1 to 15. This is the number assigned to a particular set of parameters. If no such profile of the same number exists in the system, a new profile is created with that number; otherwise, an existing set of parameters with that profile number is overwritten by the new profile.
pattern	Pattern that BERT will generate on the line.
pattern	**0s** --Repetitive pattern, all zeros.**1_in_16**--n repetitive pattern, 1 in 16.**1s**--n repetitive pattern, all ones.**211-O.152**--n pseudorandom pattern, 211 -1 O.152.**215-O.15**--n pseudorandom pattern, 215 -1 O.151.**220-O.151QRSS**--n pseudorandom pattern, 220 -1 O.151 QRSS. (This is the default.)**220-O.153**--n pseudorandom pattern, 220 -1 O.153.**3_in_24**--n repetitive pattern, 3 in 24.
threshold	Test failure (error) threshold that determines if the BERT on this line passed.
threshold	**10^-2** --Bit error rate of 10-2.**10^-3**--Bit error rate of 10-3.**10^-4**--Bit error rate of 10-4.**10^-5**--Bit error rate of 10-5.**10^-6**--Bit error rate of 10-6. (This is the default.)**10^-7**--Bit error rate of 10-7.**10^-8**--Bit error rate of 10-8.
error-injection	Error injection rate for bit errors injected into the BERT pattern generated by the chip.
err-inj	**10^-1** --Error injection of 10-1.**10^-2**--Error injection of 10-2.**10^-3**--Error injection of 10-3.**10^-4**--Error injection of 10-4.**10^-5**--Error injection of 10-5.**10^-6**--Error injection of 10-6.**10^-7**--Error injection of 10-7.**none**--No error injection in the data pattern. (This is the default.)
duration	Duration, in minutes, for which BERT is to be executed.
time	Duration of BERT, in minutes. The valid range is from 1 to 1440. The default is 10.

Command Default

The default profile created internally by the system has parameters that cannot be changed. This profile has been defined so that you can execute BERT on a line without having to configure a new profile. The default profile is displayed when the running configuration is displayed and is not stored in NVRAM:

bert profile *number* **pattern 220-0151QRSS threshold 10^-6 error-injection none duration 10**

Command Modes

Global configuration

Command History

Release	Modification
12.0(2)XD	This command was introduced.

Release	Modification
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **bert profile** command to set up bit error rate testing profiles for the Cisco AS5300 router.

The bit error rate test (BERT) feature enables you to test the quality of the connected PRI links by direct comparison of a pseudorandom or repetitive test pattern with an identical locally generated test pattern. A BERT profile is a set of parameters related to a BERT test and is stored as part of the configuration in NVRAM. You can define up to 15 BERT profiles on the system. By setting up the BERT profiles in this way, you do not have to enter the parameters each time you want to run a BERT--just select the number of the BERT profile that you want to run.

Examples

The following example shows a configured BERT profile number 1 to have a 0s test pattern, with a 10-2 threshold, no error injection, and a duration of 125 minutes:

```
Router(config)#
bert profile 1 pattern 0s threshold 10^-2 error-injection none duration 125
```

Related Commands

Command	Description
bert abort	Aborts a bit error rate testing session.
bert controller	Starts a bit error rate test for a particular port.

bitswap line

To divert the data of a disturbed transmission channel to other channels, use the **bitswap line** command in controller configuration mode. To disable bitswapping, use the **no** form of this command.

bitswap [line *line-number***]**
no bitswap [line *line-number***]**

Syntax Description

line-number	Line number. Valid values are either 0 or 1.

Command Default

Bit swapping is enabled.

Command Modes

Controller configuration (config-controller)#

Command History

Release	Modification
15.4(4)T	This command was introduced.

Usage Guidelines

- After you enable bit swapping, whenever the line conditions change, the modem swaps the bits around different channels without retraining.
- If you enable bonded mode, bit swapping will be enabled on both the lines.
- If you specify only the line number, bit swapping will be enabled only on that line.
- In case of single mode, bit swapping will be enabled only on that line.

Examples

The following example shows how to enable bit swapping on line 0:

```
Router(config-controller)# bitswap line 0
```

The following example shows how to disable bit swapping:

```
Router(config-controller)# no bitswap
```

Related Commands

Command	Description
sra line	Accommodates changes to the total link capacity with less disruption to communications.

bridge-domain

To enable RFC 1483 ATM bridging or RFC 1490 Frame Relay bridging to map a bridged VLAN to an ATM permanent virtual circuit (PVC) or Frame Relay data-link connection identifier (DLCI), use the **bridge-domain**command in Frame Relay DLCI configuration, interface configuration, interface ATM VC configuration, or PVC range configuration mode. To disable bridging, use the **no** form of this command.

bridge-domain *vlan-id* [{**access** | **dot1q** [*tag*] | **dot1q-tunnel**}] [**broadcast**] [**ignore-bpdu-pid**] [**pvst-tlv** *CE-vlan*] [**increment**] [**lan-fcs**] [**split-horizon**]
no bridge-domain *vlan-id*

Syntax Description

vlan-id	The number of the VLAN to be used in this bridging configuration. The valid range is from 2 to 4094.
access	(Optional) Enables bridging access mode, in which the bridged connection does not transmit or act upon bridge protocol data unit (BPDU) packets.
dot1q	(Optional) Enables Institute of Electrical and Electronic Engineers (IEEE) 802.1Q tagging to preserve the class of service (CoS) information from the Ethernet frames across the ATM network. If this keyword is not specified, the ingress side assumes a CoS value of 0 for quality of service (QoS) purposes.
tag	(Optional--ATM PVCs only) Specifies the 802.1Q value in the range 1 to 4095. You can specify up to 32 **bridge-domain** command entries using **dot1q***tag* for a single PVC. The highest tag value in a group of **bridge-domain** commands must be greater than the first tag entered (but no more than 32 greater).
dot1q-tunnel	(Optional) Enables IEEE 802.1Q tunneling mode, so that service providers can use a single VLAN to support customers who have multiple VLANs, while preserving customer VLAN IDs and segregating traffic in different customer VLANs.
broadcast	(Optional) Enables bridging broadcast mode on this PVC. This option is not supported for multipoint bridging. Support for this option was removed in Cisco IOS Release 12.2(18)SXF2 and Cisco IOS Release 12.2(33)SRA.
ignore-bpdu-pid	(Optional for ATM interfaces only) Ignores BPDU protocol identifiers (PIDs) and treats all BPDU packets as data packets to allow interoperation with ATM customer premises equipment (CPE) devices that do not distinguish BPDU packets from data packets.
pvst-tlv	(Optional) When the router or switch is transmitting, translates Per-VLAN Spanning Tree Plus (PVST+) BPDUs into IEEE BPDUs. When the router or switch is receiving, translates IEEE BPDUs into PVST+ BPDUs.
CE-vlan	Customer-edge VLAN in the Shared Spanning Tree Protocol (SSTP) tag-length-value (TLV) to be inserted in an IEEE BPDU to a PVST+ BPDU conversion.
increment	(PVC range configuration mode only) (Optional) Increments the bridge domain number for each PVC in the range.

lan-fcs	(Optional) Specifies that the VLAN bridging should preserve the Ethernet LAN frame checksum (FCS) of the Ethernet frames across the ATM network. **Note** This option applies only to routers using a FlexWAN module. Support for this option was removed in Cisco IOS Release 12.2(18)SXF2 and Cisco IOS Release 12.2(33)SRA.
split-horizon	(Optional) Enables RFC 1483 split horizon mode to globally prevent bridging between PVCs in the same VLAN.

Command Default

Bridging is disabled.

Command Modes

Frame Relay DLCI configuration (config-fr-dlci) Interface configuration (config-if)--Only the **dot1q** and **dot1q-tunnel** keywords are supported in interface configuration mode. Interface ATM VC configuration (config-if-atm-vc) PVC range configuration (config-if-atm-range)

Command History

Release	Modification
12.1(13)E	This command was introduced as the **bridge-vlan** command for the 2-port OC-12 ATM WAN Optical Services Modules (OSMs) on Cisco 7600 series routers and Catalyst 6500 series switches.
12.1(12c)E	This command was integrated into Cisco IOS Release 12.1(12c)E.
12.1(14)E1	This command was integrated into Cisco IOS Release 12.1(14)E1. The **dot1q-tunnel** keyword was added.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX. The **dot1q-tunnel** keyword is not supported in this release.
12.1(19)E	The **split-horizon** keyword was added.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S. The **dot1q-tunnel** and **split-horizon** keywords are supported in this release.
12.2(17a)SX	Support was added for the **dot1q-tunnel** keyword in Cisco IOS Release 12.2(17a)SX.
12.2(18)SXE	This command was renamed from **bridge-vlan** to **bridge-domain**. The **access**, **broadcast**, **ignore-bpdu-pid**, and **increment** keywords were added.
12.2(18)SXF2	Support for the **lan-fcs** and **broadcast**keywords was removed. The **ignore-bpdu-pid**and **pvst-tlv**keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

RFC 1483 bridging on ATM interfaces supports the point-to-point bridging of Layer 2 packet data units (PDUs) over Ethernet networks. RFC 1490 Frame Relay bridging on Packet over SONET (POS) or serial interfaces that are configured for Frame Relay encapsulation provides bridging of Frame Relay packets over Ethernet networks.

The Cisco 7600 router can transmit BPDUs with a PID of either 0x00-0E or 0x00-07. When the router connects to a device that is fully compliant with RFC 1483 Appendix B, in which the IEEE BPDUs are sent and received by the other device using a PID of 0x00-0E, you must not use the **ignore-bpdu-pid**keyword.

If you do not enter the **ignore-bpdu-pid** keyword, the PVC between the devices operates in compliance with RFC 1483 Appendix B. This is referred to as *strict mode* . Entering the **ignore-bpdu-pid** keyword creates *loose mode* . Both modes are described as follows:

- Without the **ignore-bpdu-pid**keyword, in strict mode, IEEE BPDUs are sent out using a PID of 0x00-0E, which complies with RFC 1483.
- With the **ignore-bpdu-pid**keyword, in loose mode, IEEE BPDUs are sent out using a PID of 0x00-07, which is normally reserved for RFC 1483 data.

Cisco-proprietary PVST+ BPDUs are always sent out on data frames using a PID of 0x00-07, regardless of whether you enter the **ignore-bpdu-pid** keyword.

Use the **ignore-bpdu-pid** keyword when connecting to devices such as ATM digital subscriber line (DSL) modems that send PVST (or 802.1D) BPDUs with a PID of 0x00-07.

The **pvst-tlv** keyword enables BPDU translation when the router interoperates with devices that understand only PVST or IEEE Spanning Tree Protocol. Because the Catalyst 6500 series switch ATM modules support PVST+ only, you must use the **pvst-tlv** keyword when connecting to a Catalyst 5000 family switch that understands only PVST on its ATM modules, or when connecting with other Cisco IOS routers that understand IEEE format only.

When the router or switch is transmitting, the **pvst-tlv** keyword translates PVST+ BPDUs into IEEE BPDUs.

When the router or switch is receiving, the **pvst-tlv** keyword translates IEEE BPDUs into PVST+ BPDUs.

Note The **bridge-domain**and **bre-connect** commands are mutually exclusive. You cannot use both commands on the same PVC for concurrent RFC 1483 and BRE bridging.

To preserve class of service (CoS) information across the ATM network, use the **dot1q** option. This configuration uses IEEE 802.1Q tagging to preserve the VLAN ID and packet headers as they are transported across the ATM network.

To enable service providers to use a single VLAN to support customers that have multiple VLANs, while preserving customer VLAN IDs and segregating traffic in different customer VLANs, use the **dot1q-tunnel** option on the service provider router. Then use the **dot1q** option on the customer routers.

Note The **access**, **dot1q**, and **dot1q-tunnel** options are mutually exclusive. If you do not specify any of these options, the connection operates in “raw” bridging access mode, which is similar to access, except that the connection does act on and transmit BPDU packets.

RFC 1483 bridging is supported on AAL5-MUX and AAL5-LLC Subnetwork Access Protocol (SNAP) encapsulated PVCs. RFC-1483 bridged PVCs must terminate on the ATM interface, and the bridged traffic must be forwarded over an Ethernet interface, unless the **split-horizon** option is used, which allows bridging of traffic across bridged PVCs.

Note RFC 1483 bridging is not supported for switched virtual circuits (SVCs). It also cannot be configured for PVCs on the main interface.

In interface configuration mode, only the **dot1q** and **dot1q-tunnel** keyword options are supported.

Examples

The following example shows a PVC being configured for IEEE 802.1Q VLAN bridging using a VLAN ID of 99:

```
Router# configure terminal

Router(config)# interface ATM6/2

Router(config-if)# pvc 2/101

Router(config-if-atm-vc)# bridge-domain 99 dot1q

Router(config-if-atm-vc)# end
```

The following example shows how to enable BPDU translation when a Catalyst 6500 series switch is connected to a device that understands only IEEE BPDUs in an RFC 1483-compliant topology:

```
Router(config-if-atm-vc)# bridge-domain
100 pvst-tlv 150
```

The **ignore-bpdu-pid** keyword is not used because the device operates in an RFC 1483-compliant topology for IEEE BPDUs.

The following example shows how to enable BPDU translation when a Catalyst 5500 ATM module is a device that understands only PVST BPDUs in a non-RFC1483-compliant topology. When a Catalyst 6500 series switch is connected to a Catalyst 5500 ATM module, you must enter both keywords.

```
Router(config-if-atm-vc)# bridge-domain
100 ignore-bpdu-pid pvst-tlv 150
```

To enable BPDU translation for the Layer 2 Protocol Tunneling (L2PT) topologies, use the following command:

```
Router(config-if-atm-vc)# bridge-domain
100 dot1q-tunnel ignore-bpdu-pid pvst-tlv 150
```

The following example shows a range of PVCs being configured, with the bridge domain number being incremented for each PVC in the range:

```
Router(config)# interface atm 8/0.100

Router(config-if)# range pvc 102/100 102/199
Router(config-if-atm-range)# bridge-domain 102 increment
```

Related Commands

Command	Description
bre-connect	Enables the BRE over a PVC or SVC.

Command	Description
show atm pvc	Displays the configuration of a particular PVC.

bridge-domain (subinterface)

To enable bridging across Gigabit Ethernet subinterfaces, use the **bridge-domain**command in subinterface configuration mode. To disable bridging, use the **no** form of this command.

bridge-domain *vlan-id* {**dot1q** | **dot1q-tunnel**} [**bpdu** {**drop** | **transparent**}] [**split-horizon**]
no bridge-domain *vlan-id* {**dot1q** | **dot1q-tunnel**} [**bpdu** {**drop** | **transparent**}] [**split-horizon**]

Syntax Description

vlan-id	Specifies the number of the virtual LAN (VLAN) to be used in this bridging configuration. The valid range is from 2 to 4094.
dot1q	Enables IEEE 802.1Q tagging to preserve the class of service (CoS) information from the Ethernet frames across the ATM network. If not specified, the ingress side assumes a CoS value of 0 for QoS purposes.
dot1q-tunnel	Enables IEEE 802.1Q tunneling mode, so that service providers can use a single VLAN to support customers who have multiple VLANs, while preserving customer VLAN IDs and keeping traffic in different customer VLANs segregated.
bpdu {**drop** | **transparent**}	(Optional) Specifies whether or not BPDUs are processed or dropped: • **drop** --Specifies that BPDU packets are dropped on the subinterface. • **transparent** --Specifies that BPDU packets are forwarded as data on the subinterface, but not processed.
split-horizon	(Optional) Enables RFC 1483 split horizon mode to globally prevent bridging between PVCs in the same VLAN.

Command Default

Bridging is disabled.

Command Modes

Subinterface configuration (config-subif)

Command History

Release	Modification
12.2(33)SRA	This command was introduced.

Usage Guidelines

This command has the following restrictions in Cisco IOS Release 12.2(33)SRA:

- The command is available on the Cisco 7600 SIP-400 with a 2-Port Gigabit Ethernet SPA only.
- You can place up to 120 subinterfaces in the same bridge domain on a single Cisco 7600 SIP-400.

To enable service providers to use a single VLAN to support customers who have multiple VLANs, while preserving customer VLAN IDs and keeping traffic in different customer VLANs segregated, use the **dot1q-tunnel** option on the service provider router. Then use the **dot1q** option on the customer routers.

Examples

The following example shows configuration of IEEE 802.1Q encapsulation for VLANs on Gigabit Ethernet subinterfaces with configuration of multipoint bridging (MPB). The MPB feature requires configuration of 802.1Q encapsulation on the subinterface.

The first subinterface bridges traffic on VLAN 100 and preserves CoS information in the packets by specifying the **dot1q** keyword.

```
Router(config)# interface GigabitEthernet 1/0/1.1
Router(config-subif)# encapsulation dot1q 10
Router(config-subif)# bridge-domain 100 dot1q
```

The second subinterface shows bridging of traffic on VLAN 200 in tunneling mode using the **dot1q-tunnel** keyword, which preserves the VLAN IDs of the bridged traffic.

```
Router(config)# interface GigabitEthernet 2/0/2.2
Router(config-subif)# encapsulation dot1q 20
Router(config-subif)# bridge-domain 200 dot1q-tunnel
```

The following example shows bridging of traffic from different VLANs on two separate Gigabit Ethernet subinterfaces into the same VLAN. First, the bridging VLAN 100 is created using the **vlan** command. Then, the Gigabit Ethernet subinterfaces implement IEEE 802.1Q encapsulation on VLAN 10 and VLAN 20 and bridge the traffic from those VLANs onto VLAN 100 using the **bridge-domain** command:

```
Router(config)# vlan 100
Router(config-vlan)# exit
!
Router(config)# interface GigabitEthernet 1/0/1.1
Router(config-subif)# encapsulation dot1q 10
Router(config-subif)# bridge-domain 100 dot1q
Router(config-subif)# exit
!
Router(config)# interface GigabitEthernet 1/0/2.1
Router(config-subif)# encapsulation dot1q 20
Router(config-subif)# bridge-domain 100 dot1q
```

Related Commands

Command	Description
encapsulation dot1q	Enables IEEE 802.1Q encapsulation of traffic on a specified subinterface in a VLAN.
vlan	Adds the specified VLAN IDs to the VLAN database and enters VLAN configuration mode.

cable bundle through clock mode

cable bundle

To configure a cable interface to belong to an interface bundle, use the **cablebundle**command in interfaceconfiguration mode. To delete a cable interface bundle definition, use the **no** form of this command.

cable bundle *number* [**master**]
no cable bundle *number* [**master**]

Syntax Description

number	Specifies the bundle identifier. Valid range is from 1 to 255.
master	(Optional) Defines the specified interface as primary.

Command Default

No cable interface bundle is defined.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1a)T1	This command was integrated into Cisco IOS Release 12.1(1a)T1.
12.0(8)SC	This command was integrated into Cisco IOS Release 12.0(8)SC
12.1(2)EC1	This command was integrated into Cisco IOS Release 12.1(2)EC1.

Usage Guidelines

You can configure up to four interface bundles. In each bundle, specify one interface as the primary interface by using the optional **master** keyword.

Configure only an IP address on the primary interface. If an IP address is configured and the interface is not specified as the primary interface, any attempt to add an interface to a bundle is rejected.

Specify all generic IP networking information (such as IP address, routing protocols, and switching modes) on the bundle primary interface. Do not specify generic IP networking information on bundle subordinate interfaces.

If you attempt to add an interface to a bundle as non-primary interface and an IP address is assigned to this interface, the command will fail. You must remove the IP address configuration before you can add the interface to a bundle.

If you have configured an IP address on a bundled interface and the interface is not the primary interface, a warning message appears.

Specify generic (not downstream or upstream related) cable interface configurations, such as source-verify or Address Resolution Protocol (ARP) handling, on the primary interface. Do not specify generic configuration on non-primary interfaces.

If you configure an interface as a part of a bundle and it is not the primary interface, all generic cable configuration for this interface is removed. The primary interface configuration will then apply to all interfaces in the bundle.

If you shut down or remove the primary interface in a bundle, no data packets are sent to any of the interfaces in this bundle. Packets are still physically received from non-primary interfaces that have not been shut down, but those packets will be discarded. Modems connected to those interfaces will not be disconnected immediately, but modems going online are not able to obtain an IP address, download their configuration file, or renew their IP address assignment if the Dynamic Host Configuration Protocol (DHCP) lease expires.

If you shut down a subordinate interface, only this interface is affected.

Examples

The following example shows how to configure interface 25 to be the primary interface:

```
Router(config-if)# cable bundle 25 master
Router(config-if)#
07:28:17: %UBR7200-5-UPDOWN: Interface Cable3/0 Port U0, changed state to down
07:28:18: %UBR7200-5-UPDOWN: Interface Cable3/0 Port U0, changed state to up
```

The following example shows the error message that appears if you try to configure an interface with an IP address that is not the primary interface:

```
Router(config-if)# cable bundle 5
Please remove ip address config first then reenter this command
```

Related Commands

Command	Description
show cable bundle	Displays the forwarding table for the specified interface bundle.

cable helper-address

To specify a destination address for User Datagram Protocol (UDP) broadcast Dynamic Host Configuration Protocol (DHCP) packets, use the **cablehelper-address**command in interface configuration mode. To remove the specified destination address for UDP DHCP packets, use the **no** form of this command.

cable helper-address *ip-address* {**cable-modem** | **host**}
no cable helper-address *ip-address* {**cable-modem** | **host**}

Syntax Description

ip-address	The IP address of a DHCP server. Based on whether you add the **host** or **cable-modem** keyword at the end of the **cablehelper-address** command, it is the IP address of the multiple service operators (MSOs) Cisco Network Registrar (CNR) server or the Internet service providers (ISPs) DHCP server.
cable-modem	Specifies that only cable modem UDP broadcasts are forwarded.
host	Specifies that only host UDP broadcasts are forwarded.

Command Default

This command is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
11.3NA	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If you specify a secondary interface address, the giaddr field in the DHCP requests will be sent to the primary address for DHCP requests received from cable modems, and to the secondary IP address for DHCP requests received from hosts.

Examples

The following example shows how to forward UDP broadcasts from cable modems to the DHCP server at 172.23.66.44:

```
Router(config-if)#
cable helper-address 172.23.66.44 cable-modem
```

The following example shows how to forward UDP broadcasts from hosts to the DHCP server at 172.23.66.44:

```
Router(config-if)# cable helper-address 172.23.66.44 host
```

cablelength

To specify the distance of the cable from the routers to the network equipment, use the **cablelength** command in controller configuration mode. To restore the default cable length, use the **no** form of this command.

cablelength *feet*
no cablelength

Syntax Description

feet	Number of feet in the range of 0 to 450.

Command Default

224 feet for a CT3IP interface processor and Clear Channel T3/E3 network module

49 feet for PA-T3 and PA-2T3 port adapters

450 feet for an interface cable between the near and far-end CSU/DSU device

Command Modes

Controller configuration

Command History

Release	Modification
11.1CA	This command was introduced.
12.2(11)YT	This command was integrated into Cisco IOS Release 12.2(11)YT and implemented on the following platforms: Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3660 series, Cisco 3725, and Cisco 3745 routers. Support for the Clear Channel T3/E3 network module was added.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

CT3IP Interface Processor and Clear Channel T3/E3 Network Module

The default cable length of 224 feet is used by the CT3IP interface processor and the Clear Channel T3/E3 network module.

PA-T3 and PA-2T3 Port Adapters

The default cable length of 49 feet is used by the PA-T3 and PA-2T3 port adapters.

Note Although you can specify a cable length from 0 to 450 feet, the hardware recognizes only two ranges: 0 to 49 and 50 to 450. For example, entering 35 feet uses the 0 to 49 range. If you later change the cable length to 40 feet, there is no change because 40 is still within the 0 to 49 range. However, if you change the cable length to 50, the 50 to 450 range is used. The actual number you enter is stored in the configuration file.

Cisco 1000 Series Router

The table below lists the cable length distances and their relationships to line buildout for E3 and T3 controllers on Cisco 1000 Series Routers:

Table 2: Cable Length Distances and Line Buildout for E3/T3 Controllers

Interface	Cable Length (Feet)	Buildout
E3	0 to 244	No line buildout
E3	225 to 450	Line buildout
T3	0 to 299	No line buildout
T3	300 to 450	Line buildout

Note Although you can specify a cable length from 0 to 450 feet, the hardware recognizes only two ranges: 0 to 49 and 50 to 450. For example, entering 35 feet uses the 0 to 49 range. If you later change the cable length to 40 feet, there is no change because 40 is still within the 0 to 49 range. However, if you change the cable length to 50, the 50 to 450 range is used. The actual number you enter is stored in the configuration file.

Examples

Cable Length to 300 Feet Example

The following example shows how to set the cable length for the router to 300 feet:

```
Router(config)#
 controller t3 9/0/0
Router(config-controller)#
 cablelength 300
```

Cisco 10000 Series Series Router Example

The following example sets the cable length to 120 feet:

```
Router(config)# controller dsx3 4/0/6
Router(config-controller)# cablelength 120
```

Related Commands

Command	Description
cablelength long	Increases the pulse of a signal at the receiver and decreases the pulse from the transmitter using pulse equalization and line buildout for a T1 cable.
cablelength short	Sets a cable length of 655 feet or shorter for a DS1 link on the Cisco MC3810 or Cisco 2600 and Cisco 3600 series routers.

cablelength (E1 controller)

To fine-tune the pulse of a signal at the receiver for an E1 cable on a Cisco AS5300 or Cisco AS5400, use the **cablelength** command in controller configuration mode. To restore the default receiver sensitivity, use the **no** form of this command.

cablelength {**custom** *gain-value* [**squelch-on**] | **long** [**squelch-on**] | **medium** [**squelch-on**] | **short** [**squelch-on**]}
no cablelength

Syntax Description

custom	Fine-tunes the receiver sensitivity for long-haul, medium-haul, and short-haul applications.
gain-value	Custom gain value for the receiver in the range of 0x1 to 0x3F. These settings are mapped to values in the range of 0 to -45 dB.
long	Fine-tunes the receiver sensitivity for long-haul applications.
medium	Fine-tunes the receiver sensitivity for medium-haul applications.
short	Fine-tunes the receiver sensitivity for short-haul applications.
squelch-on	(Optional) Enables squelch to improve the signal-to-noise ratio.

Command Default

Default receiver sensitivity for E1 cables is applied.

Command Modes

Controller configuration

Command History

Release	Modification
12.3(17)	This command was introduced.

Usage Guidelines

This command is supported on E1 controllers only.

Note The cable line pulse gain values are not dependent upon the E1 line being configured in balanced (120-ohm) mode or unbalanced (75-ohm) mode.

Examples

The following example shows how to fine-tune the receiver sensitivity for an E1 cable on a Cisco AS5300 to support a long-haul configuration:

```
Router(config-controller)# cablelength long squelch-on
```

cablelength long

To increase the pulse of a signal at the receiver and to decrease the pulse from the transmitter using pulse equalization and line build-out for a T1 cable, use the **cablelengthlong**command in controller configuration or interface configuration mode. To return the pulse equalization and line build-out values to their default settings, use the **no** form of this command.

cablelength long *db-gain-value db-loss-value*
no cablelength long

Syntax Description

db-gain-value	Number of decibels (dB) by which the receiver signal is increased. Use one of the following values: • **gain26** • **gain36** The default is 26 dB.
db-loss-value	Number of decibels by which the transmit signal is decreased. Use one of the following values: • **0db** • **-7.5db** • **-15db** • **-22.5db** The default is 0 dB.

Command Default

db-gain-value : **gain26** *db-loss-value*: **0db**

Command Modes

Controller configuration for the Cisco AS5800 and Cisco MC3810. Interface configuration for the Cisco 2600 and Cisco 3600 series routers.

Command History

Release	Modification
11.2	This command was introduced.
11.3	The following keywords were added: **gain26**, **gain36**, **0db**,**-7.5db**,**-15db**,**-22.5db**.
12.0(5)XK	This command was modified to include support as an ATM interface configuration command for the Cisco 2600 and Cisco 3600 series routers and as a controller configuration command for the Cisco AS5800 universal access server.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Cisco AS5800 and Cisco MC3810

Use this command for configuring the controller T1 interface on the Cisco AS5200 access server, on the Cisco AS5800 universal access server, or on the Cisco MC3810 multiservice access concentrator. The **cablelengthlong** command is used to configure DS1 links (meaning, to build CSU/DSU links) when the cable length is no longer than 655 feet.

On the Cisco MC3810, this command is supported on T1 controllers only and applies to Voice over Frame Relay, Voice over ATM, and Voice over HDLC.

Note On the Cisco MC3810, you cannot use the **cablelengthlong** command on a DSX-1 interface only. The **cablelengthlong** command can be used only on CSU interfaces.

A pulse equalizer regenerates a signal that has been attenuated and filtered by a cable loss. Pulse equalization does not produce a simple gain, but it filters the signal to compensate for complex cable loss. A **gain26** receiver gain compensates for a long cable length equivalent to 26 dB of loss, whereas a **gain36** compensates for 36 dB of loss.

The lengthening or *buildingout* of a line is used to control far-end crosstalk. Line build-out attenuates the stronger signal from the customer installation transmitter so that the transmitting and receiving signals have similar amplitudes. A signal difference of less than 7.5 dB is ideal. Line build-out does not produce simple flat loss (also known as *resistive* flat loss). Instead, it simulates a cable loss of 7.5 dB, 15 dB, or 22.5 dB so that the resulting signal is handled properly by the receiving equalizer at the other end.

Cisco 2600 and Cisco 3600 Series Routers

This command is supported on T1 long-haul links only. If you enter the **cablelengthlong** command on a DSX-1 (short-haul) interface, the command is rejected.

The transmit attenuation value is best obtained by experimentation. If the signal received by the far-end equipment is too strong, reduce the transmit level by entering additional attenuation.

Examples

Cisco AS5800 and Cisco MC3810

The following example shows how to increase the receiver gain by 36 decibels and decreases the transmitting pulse by 15 decibels for a long cable on a Cisco AS5800:

```
AS5800(config)# controller t1 0
AS5800(config-controller)# cablelength long gain36 -15db
```

The following example shows how to configure the cable length for controller T1 0 on a Cisco MC3810 to a decibel pulse gain of 36 decibels and a decibel pulse rate of -22.5 decibels:

```
MC3810(config)# controller t1 0
MC3810(config-controller)# cablelength long gain36 -22.5db
```

Cisco 2600 and Cisco 3600 Series Routers

On a Cisco 2600 or Cisco 3600 series router, the following example shows how to specify a pulse gain of 36 decibels and a decibel pulse rate of -7.5 decibels:

```
Router(config)#
 interface atm 0/2
Router(config-if)#
 cablelength long gain36 -7.5db
```

Related Commands

Command	Description
cablelength short	Sets a cable length of 655 feet or shorter for a DS1 link.

cablelength short

To set a cable length of 655 feet or shorter for a DS1 link on the Cisco MC3810, Cisco 2600, Cisco NCS 4200 series, and Cisco 3600 series routers, use the **cablelengthshort** command in controller configuration or interface configuration mode. To delete the **cablelengthshort** value, use the **no** form of this command.

cablelength short *length*
no cablelength short

Syntax Description

length	Specifies a cable length. Use one of the following values: • **133** --Specifies a cable length from 0 to 133 feet. • **266** --Specifies a cable length from 134 to 266 feet. • **399** --Specifies a cable length from 267 to 399 feet. • **533** --Specifies a cable length from 400 to 533 feet. • **655** --Specifies a cable length from 534 to 655 feet.

Command Default

The default is 133 feet for the Cisco AS5200 access server, Cisco AS5800 universal access server, and Cisco MC3810 multiservice access concentrator.

There is no default cable length for the Cisco 2600 and Cisco 3600 series routers.

Command Modes

Controller configuration for the Cisco AS5200 access server, Cisco AS5800 universal access server, and Cisco MC3810 multiservice access concentrator. Interface configuration for the Cisco 2600 and Cisco 3600 series routers.

Command History

Release	Modification
11.3(2)AA	This command was introduced.
12.0(5)XK	This command was modified to include support as an ATM interface command for the Cisco 2600 and 3600 series routers and as a controller configuration command for the Cisco AS5800 universal access server.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
XE 3.18SP	This command was integrated in the Cisco NCS 4200 Series. For Configuring MDL, by default setting of cablelength is short.

Usage Guidelines

Cisco AS5200 Access Server, Cisco AS5800 Universal Access Server, and Cisco MC3810 Multiservice Access Concentrator

On the Cisco MC3810, the **cablelengthshort** command is used to configure DSX-1 links when the cable length is 655 feet or less than 655 feet. On the Cisco MC3810, this command is supported on T1 controllers only.

Note On the Cisco MC3810, you cannot enter the **cablelengthshort** command on a CSU interface. The **cablelengthshort** command can be used only on DSX-1 interfaces.

Cisco 2600 and Cisco 3600 Series Routers

This command is supported on T1 short-haul links only. If you enter the **cablelengthshort** command on a long-haul interface, the command is rejected.

To set cable lengths longer than 655 feet, use the **cablelengthlong** command.

This command is supported on T1 controllers only.

Cisco AS5200 Access Server, Cisco AS5800 Universal Access Server, and Cisco MC3810 Multiservice Access Concentrator

The following example shows how to set the cable length to 266 for the T1 controller in slot 1 on dial shelf 0:

```
Router# configure terminal
Router(config)# controller t1 1/1/0
Router(config-controller)# cablelength short 266
Router(config-controller)# end
```

Cisco 2600 and Cisco 3600 Series Routers

On a Cisco 2600 or Cisco 3600 series router, the following example shows how to specify a cable length from 0 to 133 feet:

```
Router(config)#
 interface atm 0/2
Router(config-if)#
 cablelength short 133
```

Related Commands

Command	Description
cablelength long	Increases the pulse of a signal at the receiver and decreases the pulse from the sender using pulse equalization and line build-out.

card

To preprovision a router slot for an interface card, use the **card**command in global configuration mode. To remove the preprovisioning for a card, use the **no** form of this command.

card {*slot/subslot* | *slot/subslot/bay*} *card-type*
no card {*slot/subslot* | *slot/subslot/bay*} *card-type*

Cisco 10000 Series Router
card *slot/subslot* {**lchoc12-1** | **lgigethernet-l** | **1gigethernet-hh-1** | **loc12atm-1** | **loc12pos-1** | **1oc48dpt-pos-1** | **24che1t1-1** | **4chstm-1** | **4cht3-hh-1** | **4oc3atm-1** | **4oc3atm_lr-1** | **4jacket-1** | **6cht3-1** | **6oc3pos-1** | **8e3ds3-1** | **8e3ds3atm-1** | **8fastethernet-1** [**mode** {**e1** | **t1**}]*spa-type*}
no card *slot/subslot*

Cisco uBR10012 Universal Broadband Router
card {*slot* {**2jacket-1** | **4jacket-1**} | *slot/subslot* | *slot/bay*} *card-type* [**license** *license*]
no card {*slot* | *slot/subslot* | *slot/bay*} *card-type* [**license** *license*]

Syntax Description

slot/subslot	Chassis slot and subslot for the card. The following are the valid values: • *slot* --1 to 8 • *subslot* --0 or 1
slot/subslot/bay	Chassis slot and subslot for the Cisco Wideband SIP, and the bay number in the SIP where the Cisco Wideband SPA is located. The following are the valid values: • *slot* --1 to 3 • *subslot* --0 or 1 (0 is always specified) • *bay* --0 (upper bay) or 1 (lower bay) **Note** The Cisco uBR10012 router running Cisco IOS Release 12.3(21)BC supports *slot/subslot/bay* option.
slot	(Cisco uBR10012 router) Chassis slot for the Cisco SPA Interface Processor (SIP). The valid value of the *slotis*1 or 3.

slot/subslot	(Cisco uBR10012 router) Chassis slot and subslot where the Cisco Cable line card, the Timing, Communication, and Control (TCC) card, Cisco Shared Port Adaptor (SPA), or the Half-Height Gigabit Ethernet (HHGE) line card is located. **Note** Effective with Cisco IOS Release 12.2(33)SCB, the SPA slot numbering is changed to *slot*/*subslot*. For the Cisco Cable line cards, the valid values are: • *slot* --5 to 8 • *subslot* --0 or 1 For the TCC card, the valid values are: • *slot* --1 or 2 • *subslot* --1 For the HHGE line card, the valid values are: • *slot* --3 or 4 • *subslot* --0 or 1 For the SPA, the valid values are: • *slot* --0 or 3 (for SIP-600) • *slot* --1 (for Wideband SIP) • *subslot* --0 to 3
slot/bay	(Cisco uBR10012 router) Chassis slot and bay where the Cisco Shared Port Adaptor (SPA) is located. For the SPA, the valid values are: • *slot* --1 or 3 (for SIP-600) • *slot* --1 (for Wideband SIP) • *bay* --0 to 3
license	(Cisco uBR10012 router) License supported on the card. For a list of license types supported on the card, see the second table below.
card-type	Type of card for which to preprovision the slot. For a list of the supported cards, which varies by platform, see the first table below.
lchoc12-1	Preprovisions a line card slot for a 1-Port Channelized OC-12/STM-4 line card.
lgigethernet-l	Preprovisions a line card slot for a 1-Port Gigabit Ethernet line card.
1gigethernet-hh-1	Preprovisions a line card slot for a 1-Port Gigabit Ethernet Half-Height line card.
loc12atm-1	Preprovisions a line card slot for a 1-Port OC-12 ATM line card.

loc12pos-1	Preprovisions a line card slot for a 1-Port OC-12 Packet over SONET line card.
1oc48dpt-pos-1	Preprovisions a line card slot for a 1-Port OC-48/STM-16 Packet over SONET line card.
2jacket-1	(Cisco uBR10012 router) Preprovisions a slot for the Cisco Wideband SPA Interface Processor (SIP).
24che1t1-1	Preprovisions a line card slot for a 24-Port Channelized E1/T1 line card.
4chstm-1	Preprovisions a line card slot for a 4-Port Channelized OC-3/STM-1 line card.
4cht3-hh-1	Preprovisions a line card slot for a 4-port Channelized Half-Height line card.
4jacket-1	(Cisco uBR10012 router) Preprovisions a slot for the Cisco SIP-600.
4jacket-1	Preprovisions a line card slot in the Cisco 10000 series router to accept a Cisco 10000 SIP-600.
4oc3atm-1	Preprovisions a line card slot for a 4-Port OC-3/STM-1 ATM line card with intermediate-reach optics.
4oc3atm_lr-1	Preprovisions a line card slot for a 4-Port OC-3/STM-1 ATM line card with long-reach optics.
6cht3-1	Preprovisions a line card slot for a 6-Port Channelized T3 line card.
6oc3pos-1	Preprovisions a line card slot for a 6-Port OC-3/STM-1 Packet over SONET line card.
8e3ds3-1	Preprovisions a line card slot for an 8-Port Unchannelized E3/T3 line card.
8e3ds3atm-1	Preprovisions a line card slot for an 8-Port E3/DS3 ATM line card.
8fastethernet-1	Preprovisions a line card slot for an 8-Port Fast Ethernet Half-Height line card.
mode {**e1**|**t1**}	Indicates the mode of operation of the 24-Port Channelized E1/T1 line card.
spa-type	SPA type to preprovision a SPA interface.

Command Default

An empty card slot is not preprovisioned and cannot be configured or displayed.

The default mode of operation for the 24-Port Channelized E1/T1 line card is E1.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(17)ST	This command was introduced on the Cisco 10000 series routers.
12.0(21)SX	This command was integrated into Cisco IOS Release 12.0(21)SX.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.

Release	Modification
12.2(1)XF1	This command was introduced on the Cisco uBR10012 Universal Broadband Router for the following line cards: • Cisco uBR-LCP-MC28C cable interface line card • Cisco uBR-LCP-MC28C-BNC cable interface line card • Cisco uBR10-1GE Gigabit Ethernet (GigE) uplink line card • Cisco uBR10-1OC12/P-SMI OC-12 POS uplink line card
12.2(4)XF1	Support was added for the Cisco uBR-LCP-MC16C and Cisco uBR-LCP-MC16E cable interface line cards.
12.2(4)BC1	Support was added for the Cisco uBR10-SRP-OC12SML DPT WAN uplink line card.
12.2(8)BC1	Support was added for the Cisco LCP2 line card processor, and all of its combinations with the supported cable interface line cards.
12.2(11)BC3	Support was added for the Cisco uBR10012 OC-48 DPT/POS Interface Module uplink line card and Cisco uBR-MC5X20S cable interface line card.
12.2(15)BX	This command was integrated into Cisco IOS Release 12.2(15)BX.
12.2(15)CX1	Support was added for the Cisco uBR-MC16U/X and Cisco uBR-MC28U/X cable interface line cards.
12.2(15)BC2	Support was added for the Cisco uBR-MC16U/X, Cisco uBR-MC28U/X, and Cisco uBR-MC5X20U cable interface line cards.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB. This command was modified to support the 4-port Channelized Half-Height line card and the 4-Port OC-3/STM-1 ATM line card with long-reach optics by adding the 4cht3-hh-1 and the 4oc3atm_lr-1 keywords.
12.3(7)XI1	This command was integrated into Cisco IOS Release 12.3(7)XI1.
12.3(21)BC	Support was added for the Cisco Wideband SIP and Wideband SPA.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.
12.2(33)SB	This command was enhanced to provide the 4jacket-1 keyword and the spa-type option, which enable you to preprovision a line card slot to accept a Cisco 10000 SIP-600 and a SPA interface, respectively. This enhancement was implemented on the Cisco 10000 series router for the PRE3 and PRE4.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB. Support for the Cisco SIP-600 was added. This command was modified to change the addressing format for: • SIPs--From *slot/subslottoslot* • SPAs--From *slot/subslot/baytoslot/bay*

Release	Modification
12.2(33)SCC	This command was modified to support the Cisco UBR-MC20X20V cable interface line card.
12.2(33)SCE	This command was modified to support the Cisco uBR-MC3GX60V cable interface line card.
12.2(33)SCH	This command was modified to support the Cisco 3 Gbps Wideband SPA card.

Usage Guidelines

This command is supported on the Cisco uBR10012 universal broadband router and the Cisco 10000 series routers.

Use this command to preprovision a slot in the router to accept a particular line card, so that you can configure the interface without the card being physically present in the chassis. This command allows system administrators to plan for future configurations, without having to wait for the physical hardware to arrive. When the line card does arrive, the installer can bring the card online by inserting the card into the chassis and connecting the necessary cables, without having to do any further configuration using the command-line interface.

The type of card must be appropriate for the slot being specified. The list of supported card types depends on the Cisco IOS software release in use and your platform. For the latest information about supported hardware for your platform, see the release notes that correspond to your Cisco IOS software release and platform.

The table below lists the types of cards that are supported as *card-types* for the **card** command.

Table 3: Card Types Supported by the card Command

Card Type	Description
lchoc12-1	(Cisco 10000 series router) Preprovisions a line card slot for a 1-Port Channelized OC-12/STM-4 line card.
1gigethernet-1	(Cisco 10000 series and Cisco uBR10012 routers) Preprovisions a slot for a Cisco uBR10-1GE Gigabit Ethernet (GigE) uplink line card.
1gigethernet-hh-1	(Cisco 10000 series router and Cisco uBR10012 routers) Preprovisions a line card slot for a 1-Port Gigabit Ethernet Half-Height line card.
loc12atm-1	(Cisco 10000 series router) Preprovisions a line card slot for a 1-Port OC-12 ATM line card.
1oc12pos-1	(Cisco 10000 series and Cisco uBR10012 routers) Preprovisions a slot for a Cisco uBR10-1OC12/P-SMI OC-12 POS uplink line card.
1oc48dpt-pos-1	(Cisco 10000 series and Cisco uBR10012 routers) Preprovisions a slot for a Cisco uBR10012 OC-48 DPT/POS Interface Module uplink line card.
2cable-tccplus	(Cisco uBR10012 router) Preprovisions a slot for a Timing, Control, and Communications Plus (TCC+) utility card. **Note** This option is informational only, because slots 1/1 and 2/1 can be used only for the TCC+ card.
24che1t1-1	(Cisco 10000 series router) Preprovisions a line card slot for a 24-Port Channelized E1/T1 line card.

Card Type	Description
2oc12srp-sm-lr	(Cisco uBR10012 router) Preprovisions a slot for a Cisco uBR10-SRP-OC12SML DPT WAN uplink line card.
24rfchannel-spa-1	(Cisco uBR10012 router) Preprovisions a bay in the Cisco Wideband SIP for the Cisco 1-Gbps Wideband Shared Port Adapter (SPA).
4chstm-1	(Cisco 10000 series router) Preprovisions a line card slot for a 4-Port Channelized OC-3/STM-1 line card.
4cht3-hh-1	(Cisco 10000 series router) Preprovisions a line card slot for a 4-port Channelized Half-Height line card.
4oc3atm-1	(Cisco 10000 series router) Preprovisions a line card slot for a 4-Port OC-3/STM-1 ATM line card with intermediate-reach optics.
4oc3atm_lr-1	(Cisco 10000 series router) Preprovisions a line card slot for a 4-Port OC-3/STM-1 ATM line card with long-reach optics.
5cable-mc520h-d	(Cisco uBR10012 router) Preprovisions a slot for a Cisco uBR10-MC5X20H-D cable interface line card.
5cable-mc520s	(Cisco uBR10012 router) Preprovisions a slot for a Cisco uBR10-MC5X20S cable interface line card.
5cable-mc520s-d	(Cisco uBR10012 router) Preprovisions a slot for a Cisco uBR10-MC5X20S-D cable interface line card.
5cable-mc520u-d	(Cisco uBR10012 router) Preprovisions a slot for a Cisco uBR10-MC5X20U-D cable interface line card.
5cable-mc520u-f	(Cisco uBR10012 router) Preprovisions a slot for a Cisco uBR10-MC5X20U-F cable interface line card.
6cht3-1	(Cisco 10000 series router) Preprovisions a line card slot for a 6-Port Channelized T3 line card.
6oc3pos-1	(Cisco 10000 series router) Preprovisions a line card slot for a 6-Port OC-3/STM-1 Packet over SONET line card.
8e3ds3-1	(Cisco 10000 series router) Preprovisions a line card slot for an 8-Port Unchannelized E3/T3 line card.
8e3ds3atm-1	(Cisco 10000 series router) Preprovisions a line card slot for an 8-Port E3/DS3 ATM line card.
8fastethernet-1 mode {e1 | t1}	(Cisco 10000 series router) Preprovisions a line card slot for an 8-Port Fast Ethernet Half-Height line card and optionally specifies its mode of operation. E1 is the default.
ubr10k-clc-3g60	(Cisco uBR10012 router) Preprovisions a slot for a Cisco uBR-MC3GX60V cable interface line card.

Card Type	Description
ubr10k-clc-mc2020v	(Cisco uBR10012 router) Preprovisions a slot for a Cisco UBR-MC20X20V cable interface line card.
ubr10k-clc-5x20s	(Cisco uBR10012 router) Preprovisions a slot for a Cisco uBR10-MC5X20S cable interface line card.
SPA-DOCSIS-HD-V1 {**1x10GE** | **3x1GE**}	(Cisco uBR10012 router) Preprovisions a bay in the Cisco SIP-600 for the Cisco 3 Gbps Wideband SPA card.

The license supported depends on the card being specified. The list of supported license types depends on the Cisco IOS software release in use and your platform. For the latest information about supported hardware for your platform, see the release notes that correspond to your Cisco IOS software release and platform.

The table below lists the license supported by a card.

Table 4: License Supported by a card

Card Type	License Supported	Description
Cisco UBR-MC20X20V	0X20	Zero downstream and 20 upstream
	10X20	10 downstream and 20 upstream
	15X20	15 downstream and 20 upstream
	20X20	20 downstream and 20 upstream
	5X20	5 downstream and 20 upstream
	invalid	Invalid license
Cisco uBR-MC3GX60V	0 to 72	Downstream license count
	none	No license
Cisco 3 Gbps Wideband SPA	none	No license
	0 to 71	Downstream license count
	72	Downstream license count

Cisco uBR10012 Universal Broadband Router Usage Guidelines

On the Cisco uBR10012 router, you can use the **card** command to preprovision a router slot for a line card or to preprovision one or more slots for a SPA interface processor (SIP), such as the Cisco Wideband SIP. You can also use the **card** command to preprovision a SIP bay or subslot for a SPA, such as the Cisco Wideband SPA or Cisco 3 Gbps Wideband SPA.

The Cisco uBR10012 universal broadband router has the following card slot requirements:

Note Slot 0/0 is an invalid value for this command.

- Slots 1/1 and 2/1 are reserved for TCC+ utility cards. A utility card and a SPA can co-exist on a Cisco uBR10012 router with an index of 1/1.
- Slots 1/0 through 4/0 are reserved for network uplink line cards.
- Slots 1 and 3 can be used for SIPs. Each SIP occupies two physical slots in a Cisco uBR10012 router (slot pair 1/2 or slot pair 3/4). Slot 1 is recommended for the Cisco Wideband SIP.
- Slot 5/0 through 8/1 are reserved for cable interface line cards.

Tip A preprovisioned card is displayed the same way as a card physically present in the chassis. Some **show** commands might also list the preprovisioned card in their displays. In addition, using the **card** command does not change the output of the ENTITY-MIB, which displays physically and logical components installed in the router.

When a line card is inserted in the Cisco uBR10012 chassis, the router performs the following actions, depending on whether the card slot is preprovisioned for the card:

- If the inserted line card matches the type of line card preprovisioned for the slot, the system applies the preprovisioned configuration to the line card.
- If the line card slot was not preprovisioned, the system applies a basic configuration to the line card and adds that configuration to the running configuration file.
- If the line card slot was preprovisioned for one type of line card, but another type of line card has been inserted, the system replaces the preprovisioned configuration (in the running configuration file) with a basic configuration for the line card that was actually inserted. The startup configuration file is not changed.

Tip Use the **showrunning-config|includecard**command to display which slots, if any, are preprovisioned for a particular card type.

The **noversionofthe**command removes the preprovisioning information from the given card slot. This also removes all configuration information for that card slot, as well as any information in the SNMP MIB database about the card and its card slot.

Cisco 10000 Series Router Usage Guidelines

You must specify a line card slot and subslot, and the line card for which you want to preprovision the line card slot.

If you insert a line card into a line card slot that has been preprovisioned for a different line card, the line card will fail.

You can specify a mode of operation for the 24-Port Channelized E1/T1 line card. If you do not, the line card operates in the E1 mode.

In Cisco IOS releases earlier than 12.0(28)S, 12.2(16)BX, and 12.3(7)XI1, you used only the card command to change the provisioning of a line card slot. It was not necessary to remove the old line card before using the card command to change the line card provisioning.

In Cisco IOS releases after 12.0(28)S, 12.2(16)BX, and 12.3(7)XI1, you must deactivate the installed line card using the hw-module and no card commands before using the card command to provision the line card slot for a different line card. This is a general best practice when using the **card** command.

Examples

Cisco uBR10012 Universal Broadband Router Examples

The following example shows a list of supported card types, and then shows that slot 8/0 is being preprovisioned for a Cisco uBR10-MC5X20S cable interface line card. The cable interface for slot 8/0/0 can then be configured.

```
Router# config t
Router(config)# card 8/0 ?

  5cable-mc520h-d     create a uBR10000 line card with MC520H-D
  5cable-mc520s       create a uBR10000 line card with MC520S
  5cable-mc520s-d     create a uBR10000 line card with MC520S-D
  5cable-mc520u-d     create a uBR10000 line card with MC520U-D
  5cable-mc520u-f     create a uBR10000 line card with MC520U
  ubr10k-clc-3g60     create a uBR10000 line card with MC3Gx60
  ubr10k-clc-5x20s    create a uBR10000 line card with MC520S
  ubr10k-clc-mc2020v  create a uBR10000 line card with MC20x20
Router(config)# card 8/0
ubr10k-clc-5x20s
Router(config)# int c8/0/0

Router(config-if)#
```

The following example shows how to preprovision a Cisco Wideband SIP:

```
Router# configure terminal
Router(config)# card 1 2jacket-1
```

The following example shows how to preprovision a Cisco Wideband SPA on a Cisco Wideband SIP:

```
Router# configure terminal
Router(config)# card 1/0 24rfchannel-spa-1
```

The following example shows how to preprovision a Cisco SIP-600:

```
Router# configure terminal
Router(config)# card 3 4jacket-1
```

The following example shows how to preprovision a Cisco Wideband SPA on a Cisco SIP-600:

```
Router# configure terminal
Router(config)# card 3/0 24rfchannel-spa-1
```

The following example shows how to preprovision a Cisco 3 Gbps Wideband SPA on a Cisco SIP-600:

```
Router# configure terminal
Router(config)# card 1/0 SPA-DOCSIS-HD-V1 1x10GE license 1
```

Cisco 10000 Series Router Examples

The following example preprovisions line card slot 2 to accept a 24-Port Channelized E1/T1 line card operating in E1 mode:

```
Router(config)# card 2/
0 24che1t1-1
 mode e1
```

The following example shows how to change the provisioning for line card slot 5 from the 1-Port Gigabit Ethernet Half-Height line card to the 4-Port OC-3/STM-1 ATM line card.

```
Router(config)# hw-module subslot 5/0 shut
Aug 22 21:52:19.619 UTC: %IPCOIR-3-TIMEOUT: Timeout waiting for a response from slot 5/0.
Aug 22 21:52:19.619 UTC: %IPCOIR-2-CARD_UP_DOWN: Card in slot 5/0 is down.  Notifying
1gigethernet-hh-1 driver.
Aug 22 21:52:21.627 UTC: %LINK-3-UPDOWN: Interface GigabitEthernet5/0/0, changed state to
down
Aug 22 21:52:22.627 UTC: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet5/0/0,
 changed state to down
Router(config)# no card 5/0 1gigethernet-hh-1
Aug 22 21:53:20.008 UTC: %C10K-3-DEACTIVATED: card in slot [5/0] disabled.
Router(config)# card 5/0 4oc3atm-1
[ Remove the 1-Port Gigabit Ethernet Half-Height line card and
insert the 4-Port OC-3/STM-1 ATM line card ]
```

Related Commands

Command	Description
show interface	Displays the current configuration and status for a specified interface type.

card type (T1-E1)

To configure a T1 or E1 card type, use the **cardtype** command in global configuration mode. To deselect the card type on non-SPA platforms, use the **no** form of this command. The no form of this command is not available on the SPA platforms.

card type {**t1** | **e1**} *slot* [*bay*]
no card type {**t1** | **e1**} *slot* [*bay*]

Channelized T1/E1 Shared Port Adapters
card type {**t1** | **e1**} *slot* *subslot*

Syntax Description

t1	Specifies T1 connectivity of 1.544 Mbps through the telephone switching network, using AMI or B8ZS coding.
e1	Specifies a wide-area digital transmission scheme used predominantly in Europe that carries data at a rate of 2.048 Mbps.
slot	Chassis slot number. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide.
bay	(Optional) Card interface bay number in a slot (route switch processor [RSP] platform only). This option is not available on other platforms.
subslot	(Channelized T/E1 Shared Port Adapters Only) Secondary slot number on a SPA interface processor (SIP) where a SPA is installed. Refer to the platform-specific SPA hardware installation guide and the corresponding "Specifying the Interface Address on a SPA" topic in the platform-specific SPA software configuration guide for subslot information.

Command Default

No default behavior or values

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)XE	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.
12.3(1)	This command was integrated into Cisco IOS Release 12.3(1) and support was added for Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, and Cisco 3745 platforms.
12.2S	This command was integrated into Cisco IOS Release 12.2S.

Release	Modification
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE to support SPAs on the Cisco 7600 series routers and Catalyst 6500 series switches.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S to support SPAs on Cisco 12000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
XE 3.18SP	This command was integrated into Cisco NCS 4200 Series.

Usage Guidelines

Changes made using this command on non-SPA platforms, do not take effect unless the **reload** command is used or the router is rebooted.

Channelized T1/E1 Shared Port Adapters

There is no card type when the SPA is inserted for first time. The user must configure this command before they can configure individual ports.

The no form of this command is not available on the SPA platforms. To change an existing card type on SPA platforms, perform the following steps:

1. Remove the SPA from its subslot.
2. Save the configuration.
3. Reboot the router.
4. Insert the new SPA into the subslot.
5. Configure the new card using this command.

Examples

The following example configures T1 data transmission on slot 1 of the router:

```
Router(config)# card type t1 1
```

The following example configures all ports of an 8-Port Channelized T1/E1 SPA, seated in slot 5, subslot 2, in T1 mode:

```
Router(config)# card type t1 5 2
```

Related Commands

Command	Description
controller	Configures a T1 or E1 controller and enters controller configuration mode.
reload	Reloads the operating system.
show controller	Displays the controller state that is specific to controller hardware
show interface serial	Displays the serial interface type and other information.

card type (T3-E3)

To configure a T3 or E3 card type, use the **cardtype** command in global configuration mode. To deselect the card type, use the **no** form of this comand. The no form of this command is not supported on the 2-Port and 4-Port Clear Channel T3/E3 SPA on Cisco 12000 series routers.

T3 or E3 Controllers
card type {**t3** | **e3**} *slot*
no card type {**t3** | **e3**} *slot*

Clear Channel T3/E3 Shared Port Adapters
card type {**t3** | **e3**} *slot subslot*
no card type {**t3** | **e3**} *slot subslot*

Clear Channel T3/E3 Shared Port Adapters on Cisco 12000 Series Routers
card type {**t3** | **e3**} *slot subslot*

Syntax Description

t3	Specifies T3 connectivity of 44210 kbps through the network, using B8ZS coding.
e3	Specifies a wide-area digital transmission scheme used predominantly in Europe that carries data at a rate of 34010 kbps.
slot	Slot number of the interface.
subslot	(Clear Channel T3/E3 Shared Port Adapters Only) Secondary slot number on a SIP where a SPA is installed. Refer to the platform-specific SPA hardware installation guide and the corresponding "Specifying the Interface Address on a SPA" topic in the platform-specific SPA software configuration guide for subslot information.

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(11)YT	This command was integrated into Cisco IOS Release 12.2(11)YT and implemented on the following platforms: Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3660 series, Cisco 3725, and Cisco 3745 routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(1)	This command was integrated into Cisco IOS Release 12.3(1) and support was added for Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, and Cisco 3745 platforms.
12.2S	This command was integrated into Cisco IOS Release 12.2S.

Release	Modification
12.2(25)S3	This command was integrated into Cisco IOS Release 12.2(25)S3 to support SPAs on the Cisco 7304 routers.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE to support SPAs on the Cisco 7600 series routers and Catalyst 6500 series switches.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S to support SPAs on the Cisco 12000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Usage guidelines vary slightly from platform to platform as follows:

T3 or E3 Controllers

Once a card type is issued, you enter the **nocardtype** command and then another **cardtype** command to configure a new card type. You must save the configuration to the NVRAM and reboot the router in order for the new configuration to take effect.

When the router comes up, the software comes up with the new card type. Note that the software will reject the configuration associated with the old controller and old interface. You must configure the new controller and serial interface and save it.

Clear Channel T3/E3 Shared Port Adapters

To change all the SPA ports from T3 to E3, or vice versa, you enter the **nocardtype** command and then another **cardtype** command to configure a new card type.

When the router comes up, the software comes up with the new card type. Note that the software will reject the configuration associated with the old controller and old interface. You must configure the new controller and serial interface and save it.

Clear Channel T3/E3 Shared Port Adapters on Cisco 12000 Series Routers

The no form of this command is not available on the 2-Port and 4-Port Clear Channel T3/E3 SPA on Cisco 12000 series routers. To change an existing card type on Cisco 12000 series routers, perform the following steps:

1. Remove the SPA from its subslot.
2. Save the configuration.
3. Reboot the router.
4. Insert the new SPA into the subslot.
5. Configure the new card using this command.

Examples

The following example shows T3 data transmission configured in slot 1:

```
Router(config)# card type t3 1
```

The following example configures all ports of 2-Port and 4-Port Clear Channel T3/E3 SPA, seated in slot 5, subslot 2, in T3 mode:

```
Router(config)# card type t3 5 2
```

Related Commands

Command	Description
controller	Configures a T3 or E3 controller and enters controller configuration mode.
reload	Reloads the operating system.
show interface serial	Displays the serial interface type and other information.

card-protection

Use this command to configure card protection that protects traffic when the interface module is out of service, there is any software failure, or any hardware issues.

Card Protection Creation Commands:

card-protection *CPGN*

card-protection {*primary* | *backup*}

card-protection *revertive time*

Card Protection Maintenance Commands:

card-protection *CPGN* [**manual** {*primary* | *backup*} | **force** {*primary* | *backup*} | **lockout**]

Use **no card-protection** *CPGN* [**manual** {*primary* | *backup*} | **force** {*primary* | *backup*} | **lockout**] command to remove the configuration.

Syntax Description

Syntax Description:

CPGN	The card protection number 1 to 16 refers to the Card Protection Group Number (CPGN).
primary	Configures the primary card in card protection.
backup	Configures the backup card in card protection.
revertive time (Optional)	Configures card protection in revertive mode. The value ranges from 30 seconds to 720 seconds.
manual	Configures manual switch on primary or backup card in card protection. Traffic switches to selected card if there is no fault condition on that card.
force	Configures force switch on primary or backup card in card protection. Traffic switches to selected card, even if there is a fault on the card.
lockout	Configures lockout on backup card in card protection. Prevents card protection switching and forces traffic to remain on the primary card.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
XE Everest 16.7.1	This command was integarted into the Cisco NCS 4200 Series and Cisco ASR 900 Series.

Usage Guidelines

For the **manual** option, traffic switches to selected card if there is no fault condition on that card. It has lower priority than alarm and card failure. For the **force** option, traffic switches to selected card if there is fault condition. It has higher priority than manual, alarms and card failure. For the **lockout** option, it prevents card protection switching and forces traffic to remain on the primary card. The **revertive time** option has the lowest priority.

Examples

```
enable
configure terminal
card-protection [1-16]
primary slot 0 bay 0
backup slot 0 bay 5
end
card-protection 4
card-protection [manual {backup|primary} | force {backup|primary} | lockout]
end
```

Related Commands

Command	Description
show card-protection CPGN detail	Verifies the card protection configuration.

carrier-delay

To modify the default carrier delay time on a main physical interface, use the **carrier-delay** command in interface configuration or template configuration mode. To return to the default carrier delay time, use the **no** form of this command.

Conventional Carrier Delay
carrier-delay {*seconds* | **msec** *milliseconds*}
no carrier-delay

Asymmetric Carrier Delay for SIP-200- and SIP-400-Based WAN Cards on Cisco ASR 1000 Series Aggregation Services Routers
carrier-delay [{**up** | **down**}] {*seconds* | **msec** *milliseconds*}
no carrier-delay [{**up** | **down**}]

Syntax Description

seconds	For Conventional Carrier Delay: • Specifies the carrier transition delay, in seconds. The range is from 0 to 60. The default is 2. For Asymmetric Carrier Delay: • In SIP-200- and SIP-400-based WAN cards, *seconds* indicate the unit use for configuration.
msec *milliseconds*	For Conventional Carrier Delay: • Specifies the carrier transition delay, in milliseconds. The range is from 0 to 1000. For Asymmetric Carrier Delay: • In SIP-200- and SIP-400-based WAN cards, **msec** *milliseconds* indicate the unit use for configuration.
up	(Optional) Indicates that the carrier-delay configuration is for up link.
down	(Optional) Indicates that the carrier-delay configuration is for down link

Command Default

The default carrier delay (conventional) is 2 seconds.

Template configuration (config-template)

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRD	This command was modified. The **up** and **down** keywords were added.
12.2(33)SXI	This command was modified. Support for the **up** and **down** keywords was added.
Cisco IOS XE Release 2.3	This command was modified. Support for Cisco ASR 1000 Series Aggregation Services Routers was added.
15.2(2)E	This command was integrated into Cisco IOS Release 15.2(2)E. This command is supported in template configuration mode.
Cisco IOS XE Release 3.6E	This command was integrated into Cisco IOS XE Release 3.6E. This command is supported in template configuration mode.
Cisco IOS XE Fuji 16.8.x	The **up** and **down** keywords were added to the **no** form of the command

Usage Guidelines

The default carrier transition delay is 10 milliseconds on all Ethernet interfaces. This enables the carrier-delay time to ensure fast link detection.

Conventional Carrier Delay

If a link goes down and comes back before the carrier delay timer expires, the down state is effectively filtered, and the rest of the software on the router is not aware that a link-down event has occurred. Therefore, a large carrier delay timer results in fewer link-up/link-down events being detected. However, setting the carrier delay time to 0 means that *every* link-up/link-down event is detected.

In most environments a lower carrier delay is better than a higher one. The exact value that you choose depends on the nature of the link outages that you expect in your network and how long you expect those outages to last.

If data links in your network are subject to short outages, especially if those outages last less than the time required for your IP routing to converge, you should set a relatively long carrier delay value to prevent these short outages from causing disruptions in your routing tables. If outages in your network tend to be longer, you might want to set a shorter carrier delay so that the outages are detected sooner and the IP route convergence begins and ends sooner.

The following restrictions apply to carrier delay configuration:

- The Fast Link and Carrier Delay features are mutually exclusive. If you configure one feature on an interface, the other is disabled automatically.
- Administrative shutdown of an interface will force an immediate link-down event regardless of the carrier delay configuration.

Asymmetric Carrier Delay

Cisco IOS releases that support the **up** and **down** keywords allow asymmetric carrier delay (ACD) configuration. ACD allows you to configure separate delay times for link-up and link-down event notification on physical interfaces that support ACD, such as the SIP-200- and SIP-400-based interfaces. With ACD, link-up and link-down events can be notified with different delay times.

The following restrictions apply to ACD configurations:

- You cannot configure ACD on an interface if conventional carrier delay (the **carrier-delay** command without an **up** or **down** keyword) is configured on the interface.
- Link-down and link-up carrier delay times are configured in milliseconds, using the **msec** keyword, or in seconds.

Asymmetric carrier delay is supported by the following Ethernet Shared Port Adapters (SPA)s on Cisco ASR 1000 Series Aggregation Services Routers:

- SPA-1X10GE-L-V2
- SPA-2X1GE-V2
- SPA-4X1FE-TX-V2
- SPA-5X1GE-V2
- SPA-8X1GE-V2
- SPA-8X1FE-TX-V2
- SPA-10X1GE-V2

Examples

The following example shows how to change the carrier delay to 5 seconds:

```
Router(config)# interface serial2/3/0
Router(config-if)# carrier-delay 5
```

The following example shows how to change the carrier delay to 5 seconds for an interface template:

```
Device# configure terminal
Device(config)# template user-template1
Device(config-template)# carrier-delay 5
Device(config-template)# end
```

Asymmetric Carrier Delay

The following example shows how to configure a carrier delay of 8 seconds for link-up transitions and 50 milliseconds for link-down transitions:

```
Router(config)# interface GigabitEthernet2/0/0
Router(config-if)# carrier-delay up 8
Router(config-if)# carrier-delay down msec 50
```

The following example shows the output of the **show interfaces** command after the **carrier-delay** command is configured on the Gigabit Ethernet interface:

```
Router# show interfaces GigabitEthernet 0/1/0

GigabitEthernet0/1/0 is up, line protocol is up
  Hardware is SPA-8X1GE-V2, address is 001a.3046.9410 (bia 001a.3046.9410)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
```

```
   reliability 255/255, txload ½55, rxload ½55
Encapsulation ARPA, loopback not set
Keepalive not supported
Full Duplex, 1000Mbps, link type is auto, media type is 1000BaseBX10U
output flow-control is on, input flow-control is on
Asymmetric Carrier-Delay Up Timer is 4 sec
Asymmetric Carrier-Delay Down Timer is 500 msec
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
   0 packets input, 0 bytes, 0 no buffer
   Received 0 broadcasts (0 IP multicasts)
   0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
   0 watchdog, 0 multicast, 0 pause input
   0 packets output, 0 bytes, 0 underruns
   0 output errors, 0 collisions, 1 interface resets
   0 unknown protocol drops
   0 babbles, 0 late collision, 0 deferred
   0 lost carrier, 0 no carrier, 0 pause output
   0 output buffer failures, 0 output buffers swapped out
```

cem

To enter circuit emulation (CEM) configuration mode, use the **cem** command in global configuration mode.

cem *slot/port/channel*

Syntax Description

slot	Slot number in which the Circuit Emulation over IP (CEoIP) network module (NM) is installed on the networking device.
/ *port*	Port number on the CEoIP NM. The slash mark is required between the *slot* argument and the *port* argument.
/ *channel*	Channel number that identifies the channel that you want to configure (T1/E1 only). The channel number on a serial port is always 0. The slash mark is required between the *port* argument and the *channel* argument.

Command Default

CEM configuration mode is not available.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
XE 3.18SP	This command was integrated on Cisco NCS 4200 Series.
XE Everest 16.5.1	This command was integrated on Cisco NCS 4200 Series and Cisco ASR 900 Series Routers.

Usage Guidelines

Use this command to enter CEM configuration mode to allow the configuration of all CEM options.

Examples

The following example shows how to enter CEM configuration mode:

```
Router(config)# cem 1/2/0
Router(config-cem)#
```

Related Commands

Command	Description
clear cem	Clears CEM statistics.
show cem	Displays CEM statistics.

cem-group

To create a circuit emulation (CEM) channel from one or more time slots of a T1 or E1 line of an NM-CEM-4TE1 network module, use the **cem-group** command in controller configuration mode. To remove a CEM group and release the associated time slots, use the **no** form of this command.

cem-group *group-number* {**unframed** | **timeslots** *time-slot-range* [**speed** *kbps*]}
no cem-group *group-number*

cem-group *group-number* **framed**

Syntax Description

For NCS 4200 Series:

cem-group *cem-group-number* **cep**

group-number	Channel number to be used for this group of time slots. • For T1 ports, the range is from 0 to 23. • For E1 ports, the range is from 0 to 30. • For 4xC37.94 interface, only 0 group-number is supported.
unframed	Specifies that a single CEM channel is being created including all time slots and the framing structure of the line.
framed	Specifies that a single CEM channel is being created including all the timeslots and framing configured.
timeslots	Specifies that a list of time slots is to be used as specified by the *time-slot-range* argument.
time-slot-range	List of the time slots to be included in the CEM channel. The list may include commas and hyphens with no spaces between the numbers. The range of time slots supported for 4xC37.94 interface is from 1 to 12.
speed	(Optional) Specifies the speed of the channels by specifying the number of kbps of each time slot to be used. This keyword applies only to T1 channels.
kbps	(Optional) Speed of the channel, in kbps. Must be one of the following: • **56** --Specifies a speed of 56 kbps where only the seven most significant bits (MSBs) of each eight-bit time slot are used. • **64** --Specifies a speed of 64 kbps where all eight bits of each eight-bit time slot are used.
cep	Configures Circuit Emulation Service over Packet (CEP) mode.

Command Default

No CEM groups are defined.

Command Modes

Controller configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
15.1(2)SNH	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.
XE 3.18 SP	Support for this command was introduced on NCS 4200 Series.
XE Everest 16.5.1	This command was implemented on the Cisco ASR 920 Routers and Cisco NCS 4200 Series.
XE Fuji 16.8.x	The framed keyword was introduced for Cisco ASR 900 Routers and Cisco NCS 4200 Series Routrers.

Usage Guidelines

Use this command to create CEM channels on the T1 or E1 network module, NM-CEM-4TE1. A maximum of 64 channels may be created on an NM-CEM-4TE1.

Examples

The following example shows how to create circuit emulation group number 0 with a single CEM channel including all time slots and the framing structure of the line on an NM-CEM-4TE1.

```
Router(config-controller)# cem-group 0
 unframed
```

The following example shows how to create circuit emulation channel number 6 with T1 channel time slots one through four, nine, and ten using all eight bits of each time slot on an NM-CEM-4TE1.

```
Router(config-controller)# cem-group 6 timeslots 1-4,9,10
 speed 64
```

Examples

For NCS 4200 Series routers, the following example shows the configuration of CEP:

```
enable
configure terminal
controller Mediatype 0/5/0
controller sonet 0/5/0
sts-1 1
mode unframed
cem-group 100 cep
end
```

Examples

For 4-Ports C37.94 interface module, the following example shows the configuration:

```
enable
configure terminal
controller c3794 0/0/0
timeslots3
end
```

Examples

To configure framed SAToP:

```
enable
configure terminal
controller mediatype 0/5/0
mode sonet
controller sonet 0/5/0
cem-group0 framed
end
```

Related Commands

Command	Description
cem	Enters circuit emulation configuration mode.
show cem circuit	Displays the CEM statistics for the configured CEM circuits.

channel-group

To configure serial WAN on a T1 or E1 interface, use the **channel-group** command in controller configuration mode. To clear a channel group, use the **no** form of this command.

Cisco 2600 Series
channel-group *channel-group-number* **timeslots** *range* [**speed** {**56** | **64**}] [**aim** *aim-slot-number*]
no channel-group *channel-group-number*

Cisco 2611 (Cisco Signaling Link Terminal [SLT])
channel-group *channel-number*
no channel-group *channel-number*

Cisco ASR 901 Series, Cisco 2600XM Series, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, and Cisco 3745
channel-group *channel-group-number* {**timeslots** *range* [**speed** {**56** | **64**}] | **unframed**} [**aim** *aim-slot-number*]
no channel-group [*channel-group-number* **timeslots** *range*]

Cisco AS5350 and Cisco AS5400 Series
channel-group *channel-group-number*
no channel-group *channel-group-number*

Cisco MC3810
channel-group *channel-number* **timeslots** *range* [**speed** {**56** | **64**}]
no channel-group [*channel-number* **timeslots** *range*]

Syntax Description

channel-group-number	Channel-group number on the Cisco 2600 series, Cisco 2600XM, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, and Cisco 3745 routers. When a T1 data line is configured, channel-group numbers can be values from 0 to 23. When an E1 data line is configured, channel-group numbers can be values from 0 to 30. Valid values can be 0 or 1 on the Cisco AS5350 and Cisco AS5400.
timeslots *range*	Specifies one or more time slots separated by commas, and spaces or ranges of time slots belonging to the channel group separated by a dash. The first time slot is numbered 1. • For a T1 controller, the time slots range from 1 to 24. • For an E1 controller, the time slots range from 1 to 31. You can specify a time slot range (for example, 1-29), individual time slots separated by commas (for example 1, 3, 5), or a combination of the two (for example 1-14, 15, 17-31). See the "Examples" section for samples of different timeslot ranges.

speed {**56**|**64**}	(Optional) Specifies the speed of the underlying DS0s in kilobits per second. Valid values are 56 and 64. The default line speed when configuring a T1 controller is 56 kbps on the Cisco 2600 series, Cisco 2600XM series, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, Cisco 3745, and Cisco MC3810. The default line speed when configuring an E1 controller is 64 kbps on the Cisco 2600 series, Cisco 2600XM series, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, Cisco 3745, and Cisco MC3810. The line speed controls real-time (VBR-RT) traffic shaping, and the maximum burst size (MBS) is 255 cells.
aim *aim-slot-number*	(Optional) Directs HDLC traffic from the T1/E1 interface to the AIM-ATM-VOICE-30 digital signaling processor (DSP) card on the Cisco 2600 series, Cisco 2600XM series, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, and Cisco 3745.
channel-number	Number of the channel. Valid values can be 0 or 1 on the Cisco SLT (Cisco 2611).
unframed	Specifies the use of all 32 time slots for data. None of the 32 time slots is used for framing signals on the Cisco ASR 901 Series, Cisco 2600XM series, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, and Cisco 3745. This keyword is applicable to E1 only.

Command Default

The T1/E1 line is connected to the Motorola MPC-860x processor serial communication controller (SCC) or network module with two voice or WAN interface card (VIC or WIC) slots and 0/1/2 FastEthernet ports DSCC4 by default on Cisco 2600 series, Cisco 2600XM, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, and Cisco 3745 routers.

There is no default behavior or values on the Cisco SLT (Cisco 2611).

The serial interface object encapsulation is set to HDLC on a network access server (NAS) (Cisco AS5350 and Cisco AS5400 series routers).

The default line speed is 56 kbps when a T1 controller is configured on the Cisco 2600 series, Cisco 2600XM series, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, Cisco 3745, and the Cisco MC3810.

The default line speed is 64 kbps when an E1 controller is configured on the Cisco 2600 series, Cisco 2600XM series, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, Cisco 3745, and the Cisco MC3810.

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
11.3MA	This command was introduced on the Cisco MC3810.
12.0	This command was integrated into Cisco IOS Release 12.0 on the Cisco MC3810.
12.0(7)XE	This command was implemented on the Catalyst 6000 family switches.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.

Release	Modification
12.1(1)T	This command was modified to accommodate two channel groups on a port on 1- and 2-port T1/E1 multiflex voice or WAN interface cards on the Cisco 2600 and Cisco 3600 series routers.
12.1(3a)E3	The number of valid values for the *kbps*argument was changed on the Cisco MC3810; see the "Usage Guidelines" section for valid values.
12.2(11)T	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(15)T	The **aim** keyword was added for use on the Cisco 2600 series (including the Cisco 2691), Cisco 2600XM, Cisco 3660, Cisco 3725, and Cisco 3745.
12.3(1)	The **unframed** keyword was added for use on the Cisco 2600XM series, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, and Cisco 3745.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.4(3)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

Use this command to direct HDLC traffic from the T1/E1 interface to the AIM-ATM-VOICE-30 DSP card. A channel group is created using Advanced Integration Module (AIM) HDLC resources when a **channel-group** command with the **aim** keyword is parsed during system initialization or when the command is entered during configuration. You must specify the **aim** keyword under a T1/E1 controller port to direct HDLC traffic from the T1/E1 interface to the AIM-ATM-VOICE-30 DSP card on the Cisco 2600 series, Cisco 2600XM series, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, and Cisco 3745.

Note Neither the Cisco AS5400 series NAS nor the Cisco MC3810 is supported with the integrated voice and data WAN on T1/E1 interfaces using the AIM-ATM-VOICE-30 module.

If previous **channel-group** commands are configured with the **aim** keyword, subsequent **channel-group** commands without the **aim** keyword are rejected. Similarly, if a regular **channel-group** command is followed by another **channel-group** command with the **aim** keyword implemented, the second command is rejected on the Cisco 2600 and Cisco 2600XM.

A channel group using AIM HDLC resources is deleted only when a **nochannel-group** command is entered.

By default, the**channel-group** command on a NAS sets the serial interface object encapsulation to HDLC. You must override the default by entering the **encapsulationss7** command for that serial interface object. Once you override the default, encapsulation cannot be changed again for that object. The SS7 encapsulation option is new to the Integrated Signaling Link Terminal feature and is available only for interface serial objects created by the**channel-group** command. The Integrated Signaling Link Terminal feature added SLT functionality on Cisco AS5350 and Cisco AS5400 platforms.

A digital SS7 link can be deleted by entering the **nochannel-group***channel-group-number* command on the associated T1/E1 controller. The link must first be stopped using the **noshutdown** command. It is not necessary to remove the channel ID association first.

Use the **channel-group** command in configurations where the router or access server must communicate with a T1 or E1 fractional data line. The channel group number may be arbitrarily assigned and must be unique for the controller. The time-slot range must match the time slots assigned to the channel group. The service provider defines the time slots that comprise a channel group.

Note Channel groups, channel-associated signaling (CAS) voice groups, DS0 groups, and time-division multiplexing (TDM) groups all use group numbers. All group numbers configured for channel groups, CAS voice groups, and TDM groups must be unique on the local Cisco MC3810 concentrator. For example, you cannot use the same group number for a channel group and for a TDM group. Furthermore, on the Cisco MC3810, only one channel group can be configured on a controller.

The channel group number can be 0 or 1 on the Cisco SLT (Cisco 2611).

The **channel-group** command also applies to Voice over Frame Relay, Voice over ATM, and Voice over HDLC on the Cisco MC3810.

Examples

The following example shows basic configuration directing HDLC traffic from the T1/E1 interface to the AIM-ATM-VOICE-30 DSP card, starting in global configuration mode:

```
Router(config)# controller e1 1/0
Router(config-controller)# clock source internal
Router(config-controller)# channel-group 0 timeslots 1-31 aim 0
```

The following example explicitly sets the encapsulation type to PPP to override the HDLC default:

```
Router# configure terminal
Router(config)# controller t1 6/0
Router(config-controller)# channel-group 2 timeslots 3 aim 0
Router(config-controller)# exit
Router(config)# interface serial 6/0:2
Router(config-if)# encapsulation ppp
Router(config-if)# ip address 10.0.0.1 255.0.0.0
Router(config-if)# no shutdown
Router(config-if)# end
```

The following example shows how to explicitly set the encapsulation type to SS7 to override the HDLC default using the Integrated Signaling Link Terminal feature. This example uses an 8PRI DFC card inserted into slot 7, and DS0-timeslot 3 on trunk 5 of that card is used as an SS7 link:

```
Router# configure terminal
Router(config)# controller t1 7/5
Router(config-controller)# channel-group 2 timeslots 3
Router(config-controller)# exit
Router(config)# interface serial 7/5:2
Router(config-if)# encapsulation ss7
Router(config-if)# channel-id 0
Router(config-if)# no shutdown
Router(config-if)# end
```

The following example defines three channel groups. Channel-group 0 consists of a single time slot, channel-group 8 consists of seven time slots and runs at a speed of 64 kbps per time slot, and channel-group 12 consists of two time slots.

```
Router(config-controller)# channel-group 0 timeslots 1
Router(config-controller)# channel-group 8 timeslots 5,7,12-15,20 speed 64
Router(config-controller)# channel-group 12 timeslots 2
```

The following example configures a channel group on controller T1 0 on a Cisco MC3810:

```
Router(config)# controller T1 0
Router(config-controller)# channel-group 10 timeslots 10-64
```

The following example configures a channel group on controller E1 1 and specifies that all time slots are used for data:

```
controller e1 1
channel-group 1 unframed
```

Note SS7 digital F-link support for the 8PRI line card requires use of a third onboard TDM stream to route trunk DS0 messages to the onboard MGCs.

Related Commands

Command	Description
framing	Specifies the frame type for the T1 or E1 data line.
invert data	Enables channel inversion.
linecode	Specifies the line code type for the T1 or E1 line.
voice-card	Configures a card with voice processing resources and enters voice card configuration mode.
encapsulation	Sets the encapsulation type.

channel-group (interface)

To assign and configure an EtherChannel interface to an EtherChannel group, use the **channel-group** command in interface configuration mode. To remove the channel-group configuration from the interface, use the **no** form of this command.

channel-group *channel-group-number* **mode** {**active** | **on** | **passive**}
no channel-group *channel-group-number*

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers
channel-group *channel-group-number* **mode on**
no channel-group *channel-group-number*

Cisco ASR 1000 Series Routers
channel-group *channel-group-number* **mode** {**active** | **passive**}
no channel-group

Cisco Catalyst Switches
channel-group *channel-group-number* **mode** {**active** | **on** | **auto** [**non-silent**] | **desirable** [**non-silent**] | **passive**}
no channel-group *channel-group-number*

Syntax Description

channel-group-number	Integer that identifies the channel-group. Valid values are from 1 to 256; the maximum number of integers that can be used is 64. • For Fast EtherChannel groups, the number is an integer from 1 to 4. This number is the one previously assigned to the port-channel interface. • On the Cisco ASR 1000 series router, valid values are from 1 to 64.
mode	Specifies the EtherChannel mode of the interface.
active	Enables Link Aggregation Control Protocol (LACP) unconditionally.
on	Enables EtherChannel only.
auto	Places a port into a passive negotiating state in which the port responds to Port Aggregation Protocol (PAgP) packets that it receives but does not initiate PAgP packet negotiation.
non-silent	(Optional) Used with the **auto** or **desirable** mode when traffic is expected from the other device.
desirable	Places a port into an active negotiating state in which the port initiates negotiations with other ports by sending PAgP packets.
passive	Enables LACP only when an LACP device is detected.

Command Default

No channel groups are assigned.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.1CA	This command was introduced.
12.0(7)XE	Support for this command was implemented on Cisco Catalyst 6000 series switches.
12.1(3a)E3	The number of valid values for the *number*argumentwas changed; see the "Usage Guidelines" section for valid values.
12.2(2)XT	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	Support for this command was implemented on the Cisco 2600 series, the Cisco 3600 series, and the Cisco 3700 series routers and integrated into Cisco IOS Release 12.2(8)T .
12.2(14)SX	Support for this command was implemented on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was integrated into Cisco IOS Release 12.2(17d)SXB.
12.2(18)SXE	This command was changed to support advanced QinQ translation on QinQ link bundles using GE-WAN interfaces on an OSM-2+4GE-WAN+ OSM on Cisco 7600 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	Support for this command on the Cisco 7600 router was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4.

Usage Guidelines

OSMs are not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 32.

IP Address for the Physical Interface

You do not have to disable the IP address that is assigned to a physical interface that is part of a channel group, but Cisco highly recommends doing so.

Layer 2 and Layer 3 Port Channels

You can create both Layer 2 and Layer 3 port channels by entering the **interface port-channel** command or, when the channel-group gets its first physical interface assignment. The port channels are not created at run time, nor are they created dynamically.

You do not have to create a port-channel interface before assigning a physical interface to a channel group. A port-channel interface is automatically created when the channel group gets its first physical interface, if it is not already created.

Propagation of Configuration and Attribute Changes

Any configuration or attribute changes you make to the port-channel interface are propagated to all interfaces within the same channel group as the port channel. (for example, configuration changes are also propagated to the physical interfaces that are not part of the port-channel, but are part of the channel group.)

The on Keyword

When you use the **on** keyword, a usable EtherChannel exists only when a port group in on mode is connected to another port group in the on mode.

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

You do not have to create a port-channel interface before assigning a physical interface to a channel group. A port-channel interface is created automatically when the channel group gets its first physical interface, if it is not already created.

Cisco ASR 1000 Series Routers

The Cisco ASR 1000 series router has the following prerequisites and restriction:

- A port-channel must be created before member links are assigned to it.
- IP addresses must be disabled on member links before those links can be included in a port-channel.
- Fast Ethernet interfaces are not supported.

Cisco Catalyst Switches

The number of valid values for *number*depends on the software release. For software releases prior to Cisco IOS Release 12.1(3a)E3, valid values are from 1 to 256; for Cisco IOS Release 12.1(3a)E3, 12.1(3a)E4, and 12.1(4)E1, valid values are from 1 to 64. Cisco IOS Release 12.1 E and later releases support a maximum of 64 values ranging from 1 to 256.

The channel-group number is global and is shared between all the channeling protocols. If a specific channel number is used for the PAgP-enabled interfaces of a channel group, that same channel number cannot be used for configuring a channel that has LACP-enabled interfaces or vice versa.

Entering the **auto** or **desirable** keyword enables PAgP on the specified interface; the command will be rejected if it is issued on an LACP-enabled interface.

The **active** and **passive** keywords are valid on PAgP-disabled interfaces only.

You can change the mode for an interface only if it is the only interface that is designated to the specified channel group.

The **on** keyword forces the bundling of the interface on the channel without any negotiation.

You can manually configure a switch with PAgP on one side and LACP on the other side in the **on** mode.

With the **on** mode, a usable EtherChannel exists only when a port group in **on** mode is connected to another port group in **on** mode.

If you enter the **channel group** command on an interface that is added to a channel with a different protocol than the protocol you are entering, the command is rejected.

If the interface belongs to a channel, the **no** form of this command is rejected.

All ports in the same channel group must use the same protocol; you cannot run two protocols on one channel group.

PAgP and LACP are not compatible; both ends of a channel must use the same protocol.

You can change the protocol at any time, but this change causes all existing EtherChannels to reset to the default channel mode for the new protocol.

Configure all ports in an EtherChannel to operate at the same speed and duplex mode (full duplex only for LACP mode).

All ports in a channel must be on the same DFC-equipped module. You cannot configure any of the ports to be on other modules.

On systems that are configured with nonfabric-enabled modules and fabric-enabled modules, you can bundle ports across all modules, but those bundles cannot include a DFC-equipped module port.

You do not have to create a port-channel interface before assigning a physical interface to a channel group. A port-channel interface is created automatically when the channel group gets its first physical interface, if it is not already created.

You do not have to disable the IP address that is assigned to a physical interface that is part of a channel group, but it is highly recommended.

You can create both Layer 2 and Layer 3 port channels by entering the **interface port-channel** command or when the channel group gets its first physical interface assignment. The port channels are not created at runtime or dynamically.

Any configuration or attribute changes that you make to the port-channel interface are propagated to all interfaces within the same channel group as the port channel (for example, configuration changes are also propagated to the physical interfaces that are not part of the port channel but are part of the channel group).

When configuring Layer 2 EtherChannels, you cannot put Layer 2 LAN ports into manually created port-channel logical interfaces.

Only the **on** mode is supported when using this command with GE-WAN ports on the OSM-2+4GE-WAN+ OSM to create QinQ link bundles for advanced QinQ translation. Also, you cannot use the **channel-group** command on GE-WAN interfaces if MPLS is configured. You must remove all IP, MPLS, and other Layer 3 configuration commands before using the **channel-group** command with GE-WAN interfaces.

Note The GE-WAN interfaces on an OSM-2+4GE-WAN+ OSM behave slightly differently than other interfaces if you want to move the interface from one group to another. To move most other interfaces, you can enter the **channel-group** command again to delete the interface from the old group and move it to the new group. For GE-WAN ports, however, you must manually remove the interface from the group by entering the **no channel-group** command before assigning it to a new group.

Caution Do not enable Layer 3 addresses on the physical EtherChannel interfaces. Assigning bridge groups on the physical EtherChannel interfaces causes loops in your network.

For a complete list of guidelines, see the "Configuring EtherChannel" section of the *Cisco 7600 Series Router Cisco IOS Software Configuration Guide*.

Fast EtherChannel

Before you assign a Fast Ethernet interface to a Fast EtherChannel group, you must first create a port-channel interface. To create a port-channel interface, use the **interface port-channel** global configuration command.

If the Fast Ethernet interface has an IP address assigned, you must disable it before adding the Fast Ethernet interface to the Fast EtherChannel. To disable an existing IP address on the Fast Ethernet interface, use the **no ip address**command in interface configuration mode.

The Fast EtherChannel feature allows multiple Fast Ethernet point-to-point links to be bundled into one logical link to provide bidirectional bandwidth of up to 800 Mbps. Fast EtherChannel can be configured between Cisco 7500 series routers and Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI) or between a Cisco 7500 series router or a Cisco 7000 series router with the RSP7000 and RSP700CI and a Cisco Catalyst 5000 switch.

A maximum of four Fast Ethernet interfaces can be added to a Fast EtherChannel group.

Caution The port-channel interface is the routed interface. Do not enable Layer 3 addresses on the physical Fast Ethernet interfaces. Do not assign bridge groups on the physical Fast Ethernet interfaces because it creates loops. Also, you must disable spanning tree.

To display information about the Fast EtherChannel, use the **show interfaces port-channel**EXEC command.

For more guidelines see the “Configuring EtherChannel” section of the *Cisco 7600 Series Router Cisco IOS Software Configuration Guide* and the “Configuring EtherChannel” section of the *Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide*

Examples

This example shows how to add EtherChannel interface 1/0 to the EtherChannel group that is specified by port-channel 1:

```
Router(config-if)#
channel-group 1 mode on
Router(config-if)#
```

The following example shows how to add interface Fast Ethernet 1/0 to the Fast EtherChannel group specified by port-channel 1:

```
Router(config)#
interface port-channel 1
Router(config-if)#
exit
Router(config)#
interface fastethernet 1/0
Router(config-if)#
channel-group 1
```

Related Commands

Command	Description
interface	Creates a port-channel virtual interface and puts the CLI in interface configuration mode when the **port-channel** keyword is used.
ip address	Sets a primary or secondary IP address on an interface.
show etherchannel	Displays the EtherChannel information for a channel.
show interfaces port-channel	Displays traffic that is seen by a specific port channel.

channel-protocol (interface)

To enable Port Aggretation Control Protocol (PAgP) or Link Aggregation Control Protocol (LACP) on an interface to manage channeling, use the**channel-protocol** command in interface configuration mode. Use the **no** form of this command to deselect the protocol.

channel-protocol {**lacp** | **pagp**}
no channel-protocol

Syntax Description

lacp	Specifies LACP to manage channeling.
pagp	Specifies PAgP to manage channeling.

Command Default

pagp

Command Modes

Interface configuration

Command History

Release	Modification
10.2	This command was introduced.
12.1(11b)EX	Support for this command was introduced on the Catalyst 6500 series switches.
12.1(12c)EA1	Support for this command was introduced on the Catalyst 2900 series switches.
12.1(13)E	Support for this command on the Catalyst 6500 series switches was extended to Cisco IOS Release 12.1(13)E. This command was changed to support the use of the **nochannel-protocol** command (without arguments) to deselect the protocol.
12.1(13)EW	Support for this command was introduced on the Catalyst 4500 series switches.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is valid on multiple interfaces (for example, Fast Ethernet) and routers and switches including the Cisco 2900, 4500/4000, 6500/6000, and 7600 series.

Examples

The following example shows how to set the lacp.

```
(config-if)# channel-protocol lacp
```

channelized

To configure the T3/E3 controller for channelized mode, use the **channelized** command in controller configuration mode. To configure the T3/E3 controller for unchannelized mode, use the**no** form of this command.

channelized
no channelized

Syntax Description

This command has no arguments or keywords.

Command Default

The T3 controller is channelized.

The E3 controller is channelized.

Maximum transmission unit (MTU) size is set to 1500.

MTU size is set to 4470.

Command Modes

Controller configuration

Command History

Release	Modification
12.0(14)S	This command was introduced.
12.1(5a)E	This command was integrated into Cisco IOS Release 12.1(5a)E.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
XE 3.18SP	This command was integrated into Cisco NCS 4200 Series.
XE Everest 16.5.1	This command was integrated into Cisco NCS 4200 Series.

Usage Guidelines

Use the no channelized controller configuration command to configure the T3/E3 controller for unchannelized mode for Cisco NCS 4200 Series. When you configure the PA-MC-2T3+ port adapter on a Cisco 7500 series router with the no channelized command, the MTU size is set to 4470. In channelized mode, the default MTU size is 1500. The change in MTU sizes will cause a memory recarve and CBus complex to occur, disrupting all traffic on the router for several minutes.

The following message will be displayed when commands initiate switching between channelized and unchannelized modes on a Cisco 7500 series router:

```
Change to subrate mode will cause cbus complex reset. Proceed? [yes/no]:
Y
```

Type Y for “yes” at the end of the warning. At the prompt, type ^Z to exit. You will exit configuration mode and enter unchannelized mode.

Caution The no channelized command removes all channel groups from a channelized T3 interface. If you have already configured channel groups, use this command with caution.

Examples

Cisco 7500 Series Router

The following example shows how to configure unchannelized mode on a PA-MC-2T3+ port adapter in slot 1 of a Versatile Interface Processor version 2 (VIP2) or VIP4 in a Cisco 7500 series router:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# controller T3 1/1/0
Router(config-controller)# no channelized
Change to subrate mode will cause cbus complex reset. Proceed? [yes/no]:
Y
^Z
```

Cisco 10000 Series Router

The following example eliminates the T1 interfaces to create a full-rate T3 interface:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# controller T3 2/0/0
Router(config-controller)# no channelized
Router(config-controller)# exit
Router(config)#
```

Cisco NCS 4200 Series

The following example shows how to configure channelized controller as T3 interface.

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# controller T3 0/4/40
Router(config-controller)# channelized
```

The following example shows how to configure channelized controller as E3 interface.

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# controller E3 0/4/40
Router(config-controller)# channelized mode e1
```

class cem

To configure CEM interface parameters in a class that is applied to CEM interfaces together, use the **class cem** command in global configuration mode. This command works in the same manner for CEM interfaces as the pseudowire-class command does for xconnect.

class cem *class name*

Syntax Description

Syntax Description

class name	The name of a CEM interface parameters class.

Command Default

CEM configuration mode is not available.

Command Modes

Global configuration

Command History

Release	Modification
XE 3.18 SP	Support for this command was introduced on NCS 4200 Series.
XE Everest 16.5.1	This command was integrated into the Cisco NCS 4200 Series and Cisco ASR 900 Series Routers.

Usage Guidelines

The **class cem** command allows you to configure CEM interface parameters in a class that is applied to CEM interfaces together. A class cem command includes the following configuration settings:

- dejitter-buffer dejitter-in-ms
- idle-pattern 8-bit-idle-pattern
- payload-size payload-size-in-ms

Note The **rtp-present** command cannot be configured from **class cem** and has to be configured from the interface for NCS 4200 Series routers.

Note You can improve the performance of packet reordering on TDM/PWE connections by using the increasing the size of the dejitter buffer using the dejitter-buffer parameter.

Examples

The following example shows how to enter CEM interface parameters:

```
enable
configure terminal
class cem mycemclass
payload-size 512
dejitter-buffer 10
idle-pattern 0x55
```

```
exit
interface cem 0/0
no ip address
cem 0
cem class mycemclass
xconnect 10.10.10.10 200 encapsulation mpls
exit
```

Related Commands

Command	Description
clear cem	Clears CEM statistics.
show cem	Displays CEM statistics.

clear aim

To clear the data compression Advanced Interface Module (AIM) daughter card registers and reset the hardware, use the **clearaim** command in privileged EXEC mode.

clear aim *element-number*

Syntax Description

element-number	Number of AIM slot. AIM slots begin with 0.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **clearaim**command is used to reset the data compression AIM hardware. This command is used if the compression Advanced Interface Module (CAIM) hardware becomes "stuck" or hangs for some reason. The CAIM registers are cleared, and the hardware is reset upon execution. All compression history is lost when the CAIM is reset.

This command is supported only on Cisco 2600 series routers.

Examples

The following example shows how to use the **clearaim** command. This command will reset the hardware, flushing the buffers and history for all compression tasks currently under operation:

```
Router# clear aim 0
Router#
1w0d: %CAIM-6-SHUTDOWN: CompressionAim0 shutting down
1w0d: %CAIM-6-STARTUP: CompressionAim0 starting up
```

Related Commands

Command	Description
show pas caim	Displays the IDPROM contents for each AIM board in the Cisco 2600 series routers.
test aim eeprom	Tests the data compression AIM after it is installed in a Cisco 2600 series router.

clear cable-diagnostics tdr

To clear a specific interface or clear all interfaces that support Time Domain Reflectometry (TDR), use the **clearcable-diagnosticstdr**command in privileged EXEC mode.

clear cable-diagnostics tdr [**interface** *interface* *interface-number*]

Syntax Description

interface *interface*	(Optional) Specifies the interface type; possible valid values are **ethernet**, **fastethernetgigabitethernet**, and **tengigabitethernet**. See the "Usage Guidelines" section for additional valid values.
interface-number	Module and port number; see the "Usage Guidelines" section for valid values.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(17a)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The valid values for *interface* include the**ge-wan**, **atm**, and **pos** keywords that are supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

See the *Release Notes for Cisco IOS Release 12.2 SX on the Catalyst 6500 and Cisco 7600 Supervisor Engine 720, Supervisor Engine 32, and Supervisor Engine 2* for the list of modules that support TDR

Examples

This example shows how to clear a specific interface:

```
Router# clear cable-diagnostics tdr interface gigabitethernet 4/1
Router#
```

Related Commands

Command	Description
show cable-diagnostics tdr	Displays the test results for the TDR cable diagnostics.
test cable-diagnostics	Tests the condition of 10-Gigabit Ethernet links or copper cables on 48-port 10/100/1000 BASE-T modules.

clear catalyst6000 traffic-meter

To clear the traffic meter counters, use the **clear catalyst6000 traffic-meter**command in privileged EXEC mode.

clear catalyst6000 traffic-meter

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(17a)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to clear the traffic meter counters:

```
Router# clear catalyst6000 traffic-meter
Router#
```

clear cem

To clear circuit emulation (CEM) statistics, use the **clearcem** command in privileged EXEC mode.

clear cem {*slot* | *slot*/*port*/*channel* | **all**}

Syntax Description

slot	Clears the statistics for all CEM channels on the card in the specified slot (if the card is a Circuit Emulation over IP [CEoIP] card).
slot	Specifies the slot of the CEM channel to clear.
/ *port*	Specifies the port of the CEM channel to clear. The slash mark is required between the *slot* argument and the *port* argument.
/ *channel*	Specifies the CEM channel to clear. The slash mark is required between the *port* argument and the *channel* argument.
all	Clears the statistics for all CEM channels on the router.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.

Examples

The following example shows how to clear CEM statistics for CEM channel number 10 on the card installed in slot 1, port 1.

```
Router# clear cem 1/1/10
```

Related Commands

Command	Description
cem	Enters CEM configuration mode.
show cem	Displays CEM statistics.

clear controller

To reset the T1 or E1 controller, use the **clearcontroller**command in user EXEC or privileged EXEC mode.

Cisco 7200 Series and Cisco 7500 Series Routers
clear controller {**t1** | **e1**} *slot/port*

Cisco AS5200 Series and Cisco AS5300 Series Routers
clear controller {**t1** | **e1**} *number*

Syntax Description

t1	T1 controller.
e1	E1 controller.
slot / *port*	Backplane slot number and port number on the interface. Refer to your hardware installation manual for the specific slot and port numbers.
number	Network interface module (NIM) number, in the range from 0 to 2.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
10.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example resets the T1 controller at slot 4, port 0 on a Cisco 7500 series router:

```
Router# clear controller t1 4/0
```

The following example resets the E1 controller at NIM 0:

```
Router# clear controller e1 0
```

Related Commands

Command	Description
controller	Configures a T1, E1, or J1 controller and enters controller configuration mode.

clear controller lex

To reboot the LAN Extender chassis and restart its operating software, use the **clearcontrollerlex** command in privileged EXEC mode.

clear controller lex *number* [**prom**]

Cisco 7500 Series
clear controller lex *slot/port* [**prom**]

Cisco 7200 Series and 7500 Series with a Packet over SONET Interface Processor
clear controller lex [*type*] *slot/port*

Cisco 7500 Series with Ports on VIP Cards
clear controller lex [*type*] *slot/port-adapter/port*

Syntax Description

number	Number of the LAN Extender interface corresponding to the LAN Extender to be rebooted.
prom	(Optional) Forces a reload of the PROM image, regardless of any Flash image.
slot	Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information.
port	Number of the port being configured. Refer to the appropriate hardware manual for slot and port information.
type	(Optional) Specifies the interface type. See Table 4 under the **clearcounters** command for keywords.
port-adapter	Number of the port adapter being configured. Refer to the appropriate hardware manual for information about port adapter compatibility.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(15)T	This command is no longer supported in Cisco_IOS Mainline or Technology-based (T) releases. It may continue to appear in Cisco_IOS 12.2S-family releases.

Usage Guidelines

The **clearcontrollerlex** command halts operation of the LAN Extender and performs a cold restart.

Without the **prom** keyword, if an image exists in Flash memory, and that image has a newer software version than the PROM image, and that image has a valid checksum, then this command runs the Flash image. If any one of these three conditions is not met, this command reloads the PROM image.

With the **prom** keyword, this command reloads the PROM image, regardless of any Flash image.

Examples

The following example halts operation of the LAN Extender bound to LAN Extender interface 2 and causes the LAN Extender to perform a cold restart from Flash memory:

```
Router#
clear controller lex 2
reload remote lex controller? [confirm] yes
```

The following example halts operation of the LAN Extender bound to LAN Extender interface 2 and causes the LAN Extender to perform a cold restart from PROM:

```
Router#
clear controller lex 2 prom
reload remote lex controller? [confirm] yes
```

clear controller wanphy

T o clear the triggered alarm counters for the Cisco 1-Port 10 Gigabit Ethernet LAN/WAN-PHY Shared Port Adapter and reset it to zero, use the **clearcontrollerwanphy**commandin Privileged EXEC mode.

clear controller wanphy *slot/subslot/port*

Syntax Description

slot	The SIP slot number in which the Cisco 1-Port 10 Gigabit Ethernet LAN/WAN-PHY Shared Port Adapter has been installed.
subslot	The subslot number in which the Cisco 1-Port 10 Gigabit Ethernet LAN/WAN-PHY Shared Port Adapter has been installed.
port	The port number of the Cisco 1-Port 10 Gigabit Ethernet LAN/WAN-PHY Shared Port Adapter. **Note** There is only 1 port (0) in the Cisco 1-Port 10 Gigabit Ethernet LAN/WAN-PHY Shared Port Adapter.

Command Default

No default values are available.

Command Modes

Privileged EXEC Mode (EXEC)

Command History

Release	Modification
Cisco IOS XE Release 3.3.0S	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines

The **clearcontrollerwanphy**command has been introduced on the Cisco ASR 1000 Series Router in Cisco IOS XE Release 3.3.0S. This command is used to clear the counter of alarms generated, and reset it back to zero.

Examples

The following example shows the output of the **showcontrollerswanphy** command. The example shows the alarm counter values for the line, path, and section alarms:

```
Router# show controllers wanphy 0/1/0
TenGigabitEthernet0/1/0
Mode of Operation: WAN Mode
SECTION
  LOF = 1              LOS    = 0                            BIP(B1) = 22
LINE
  AIS = 1              RDI    = 0           FEBE = 0         BIP(B2) = 3099
PATH
  AIS = 1              RDI    = 0           FEBE = 4         BIP(B3) = 4
  LOP = 0              NEWPTR = 0           PSE  = 0         NSE     = 0
WIS ALARMS
  SER    = 1           FELCDP = 0           FEAISP = 0
  WLOS   = 0           PLCD   = 0
  LFEBIP = 857         PBEC   = 4
Active Alarms[All defects]: None
Active Alarms[Highest Alarms]: None
Alarm reporting enabled for: SF SWLOF B1-TCA B2-TCA PLOP WLOS
  Rx(K1/K2): 00/00  Tx(K1/K2): 00/00
  S1S0 = 00, C2 = 0x1A
```

```
PATH TRACE BUFFER: STABLE
  Remote J1 Byte : wert
BER thresholds:  SD = 10e-6  SF = 10e-3
TCA thresholds:  B1 = 10e-6  B2 = 10e-6  B3 = 10e-6
[Output is Cut]
```

The following example shows how to clear the alarm counter values and reset it back to zero:

```
Router# clear controller wanphy 0/1/0
```

The following example shows that the alarm counter values are cleared and have been reset to zero:

```
Router# show controllers wanphy 0/1/0
TenGigabitEthernet0/1/0
Mode of Operation: WAN Mode
SECTION
  LOF = 0             LOS    = 0                            BIP(B1) = 0
LINE
  AIS = 0             RDI    = 0          FEBE = 0          BIP(B2) = 0
PATH
  AIS = 0             RDI    = 0          FEBE = 0          BIP(B3) = 0
  LOP = 0             NEWPTR = 0          PSE  = 0          NSE     = 0
WIS ALARMS
  SER    = 0          FELCDP = 0          FEAISP = 0
  WLOS   = 0          PLCD   = 0
  LFEBIP = 0          PBEC   = 0
```

Related Commands

Command	Description
show controllers wanphy	Displays the SPA mode (LAN/WAN), alarms, and J1 byte string value.

clear controller vdsl

To reset the VDSL line related counters, use the **clearcontrollervdsl** command in privileged EXEC mode.

clear controller vdsl *slot/subslot/port number*

Syntax Description

vdsl	VDSL2 controller.
slot	Controller slot number.
subslot	Controller subslot number.
port number	Controller port number.

Command Default

None.

Command Modes

Privileged EXEC mode.

Command History

Release	Modification
15.0(1)M1	This command was first introduced.

Usage Guidelines

None.

Examples

The following example shows how to reset the VDSL line related counters.

```
Router#clear controller vdsl 0/2/0
```

Related Commands

Command	Description
show controller vdsl	Displays VDSL controller related information.

clear counters

To clear the interface counters, use the **clearcounters** command in user EXEC or privileged EXEC mode.

clear counters commandclear counters [*interface-type interface-number*]

Cisco 7200 Series and 7500 Series with a Packet over SONET Interface Processor
clear counters [*interface-type*] *slot/port*

Cisco 7500 Series with Ports on VIP Cards
clear counters [*interface-type*] *slot/port-adapter/port*

Cisco 7600 Series
clear counters [{*interface interface-number* | **null** *interface-number* | **port-channel** *number* | **vlan** *vlan-id*}]

Syntax Description

interface-type	(Optional) Specifies the interface type; one of the keywords listed in Table 1 .
interface -number	(Optional) Specifies the interface number displayed with the **showinterfaces** command.
slot	Slot number. Refer to the appropriate hardware manual for slot and port information.
port	Port number. Refer to the appropriate hardware manual for slot and port information.
port-adapter	Port adapter number. Refer to the appropriate hardware manual for information about port adapter compatibility.
interface	(Optional) Interface type; possible valid values are **ethernet**, **fastethernetgigabitethernet**, and **tengigabitethernet**. See the "Usage Guidelines" section for additional valid values.
interface-number	(Optional) Module and port number; see the "Usage Guidelines" section for valid values.
null *interface-number*	(Optional) Specifies the null interface; the valid value is **0**.
port-channel *number*	(Optional) Specifies the channel interface; valid values are a maximum of 64 values ranging from 1 to 256.
vlan *vlan-id*	(Optional) Specifies the VLAN ID; valid values are from 1 to 4094.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
11.2F	The **virtual-access** keyword was added.

Release	Modification
11.3	The following keywords were added or modified: • **vg-anylan** keyword was added. • **posi** keyword was changed to **pos**.
12.2(15)T	The **ethernet** and **serial** keywords were removed because the LAN Extension feature is no longer available in Cisco IOS software.
12.2(17a)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command clears all the current interface counters from the interface unless the optional arguments *interface*-type and *interface*-numberare specified to clear only a specific interface type (serial, Ethernet, Token Ring, and so on). The table below lists the command keywords and their descriptions.

Note This command does not clear counters retrieved using Simple Network Management Protocol (SNMP), but only those seen with the **showinterface** command. However, variables seen with the **showinterface** command that could affect routing, such as load and reliability, or non-cumulative variables, such as input or output rates, are not cleared.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

Table 5: clear counters Interface Type Keywords

Keyword	Interface Type
async	Asynchronous interface
bri	ISDN BRI
dialer	Dialer interface
ethernet	Ethernet interface
fast-ethernet	Fast Ethernet interface
fddi	FDDI
hssi	High-Speed Serial Interface (HSSI)
line	Terminal line

Keyword	Interface Type
loopback	Loopback interface
null	Null interface
port-channel	Port channel interface
pos	Packet OC-3 interface
serial	Synchronous serial interface
switch	Switch interface
tokenring	Token Ring interface
tunnel	Tunnel interface (IEEE 02.5)
vg-anylan	100VG-AnyLAN port adapter
virtual-access	Virtual-access interface (Refer to the *Cisco IOS Dial Technologies Command Reference* for details on virtual templates.)
virtual-template	Virtual-template interface (Refer to the *Cisco IOS Dial Technologies Command Reference* for details on virtual templates.)
virtual-tokenring	Virtual Token Ring interface

Examples

The following example shows how to clear all interface counters:

```
Router#
 clear counters
```

The following example shows how to clear the Packet OC-3 interface counters on a POSIP card in slot 1 on a Cisco 7500 series router:

```
Router#
 clear counters pos 1/0
```

The following example shows how to clear the interface counters on a Fast EtherChannel interface:

```
Router# clear counter port-channel 1
Clear "show interface" counters on all interfaces [confirm] Y
%CLEAR-5-COUNTERS: Clear counter on all interfaces by console 1
```

Related Commands

Command	Description
show interfaces	Displays the statistical information specific to a serial interface.
show interfaces port-channel	Displays the information about the Fast EtherChannel on Cisco 7500 series routers and Cisco 7000 series routers with the RSP7000 and RSP7000CI.
show queueing interface	Displays queuing information.

clear debug platform condition all

To remove the debug conditions applied to a platform, use the **clear debug platform condition all** command in privileged EXEC mode.

clear debug platform condition all

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.10.0S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

The following example shows how to remove the conditional debugging applied to the platform.

```
Router# clear debug platform condition all
```

clear diagnostic event-log

To clear the diagnostic event logs for a specific module or event type, use the **cleardiagnosticevent-log**command in Priveleged exec mode.

clear diagnostic event-log {**event-type** {**error** | **info** | **warning**} | **module** {**num** | *slot subslot* | **all**}}

Syntax Description

event-type error	Specifies clearing error events.
event-type info	Specifies clearing informative events.
event-type warning	Specifies clearing warning events.
module *num* | *slotsubslot*	Specifies clearing events for a specific module.
module all	Specifies clearing all linecards.

Command Default

This command has no default settings.

Command Modes

Priveleged Exec mode(#)

Command History

Release	Modification
12.2(33)SXH	This command was introduced on the Supervisor Engine 720.

Usage Guidelines

The **cleardiagnosticevent-log** command clears all the events for all the modules.

The **cleardiagnosticevent-logmodule***num* command clears events only for a specific module.

The **cleardiagnosticevent-logevent-type**command clears only specific event types such as error, informative, or warning events.

Examples

This example shows how to clear error event logs:

```
Router# clear diagnostic event-log event-type error
```

This example shows how to clear event logs on module 3:

```
Router# clear diagnostic event-log module 3
```

This example shows how to clear error event logs on all the modules:

```
Router# clear diagnostic event-log module all
```

Related Commands

Command	Description
show diagnostic events	Displays the diagnostic event log

clear dsip tracing

To clear Distributed System Interconnect Protocol (DSIP) tracing statistics (trace logging), use the **cleardsiptracing** command in privileged EXEC mode.

clear dsip tracing {**counters** | **tracing**} [{**control** | **data** | **ipc**}]

Syntax Description

counters	DSIP counters.
tracing	DSIP tracing buffers.
control	(Optional) Control counters or tracing buffers.
data	(Optional) Data counters or tracing buffers.
ipc	(Optional) Inter-process communication counters or tracing buffers.

Command Default

If no option is specified, all control, data, and inter-process communication counters or tracing buffers are cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to clear the counters displayed with the **showdsiptracing** EXEC command.

Examples

In the following example, the DSIP counters are cleared (including data, control, and ipc counters):

```
Router# clear dsip tracing
```

Related Commands

Command	Description
show dsip tracing	Displays DSIP tracing buffer information.
show dsip version	Displays DSIP version information.

clear facility-alarm

To clear alarm conditions and reset the alarm contacts, use the **clearfacility-alarm**command in privileged EXEC mode.

clear facility-alarm [{**critical** | **major** | **minor** | **source pem** {**0** | **1**}}]

Syntax Description

critical	(Optional) Clears all critical alarms.
major	(Optional) Clears all major alarms.
minor	(Optional) Clears all minor alarms.
source pem {**0** | **1**}	(Optional--Cisco uBR10012 only) Clears all alarms for either the first or second Power Entry Module (PEM).

Command Default

If specified without any options, clears all facility alarms with the exception of:

- An alarm that illuminates the CRIT, MIN, or MAJ LED
- A visual alarm (DC lightbulb) that is wired to the DB-25 connector on a power supply

If specified without any options, clears all facility alarms.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(17)SL	This command was introduced on the Cisco 10000 series router.
12.2(1)XF1	This command was introduced for the Cisco uBR10012 router.
12.2(16)BX	This command was introduced on the PRE2.
12.2(31)SB2	This command was introduced on the PRE3 for the Cisco 10000 series router.
12.3BC	This command was integrated into Cisco IOS Release 12.3BC.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 on the Cisco ASR 1000 Series Routers.

Usage Guidelines

Cisco ASR 1000 Series Routers

The clear facility-alarm command clears audible alarms. A recurrence of the original alarm source after the original alarm condition is removed restarts the audible alarm.

The clear facility-alarm command does not clear an alarm that illuminates the CRIT, MIN, or MAJ LED. This command does not turn off a visual alarm (DC light bulb) that is wired to the DB-25 connector on a power supply.

To clear a CRIT, MIN, or MAJ alarm LED or a visual alarm, you must resolve the alarm condition. For example, if a critical alarm LED is illuminated because an active SPA was removed without a graceful deactivation of the SPA, the only way to resolve that alarm is to replace the SPA.

Cisco uBR10012 Universal Broadband Router

The **clearfacility-alarm** command clears the contacts to an external alarm panel. Only a recurrence of the original alarm source after the original alarm condition is removed can restart the audible alarm. These alarms are displayed by the **showfacility-alarmstatus**command.

The alarm LEDs remain lit on the Performance Routing Engine (PRE) as long as the alarm condition continues and is not cleared by the **clearfacility-alarm** command. An alarm can only be removed from the list by correcting the issue that is triggering the alarm.

Examples

The following example shows how to clear all facility alarms on the router:

```
Router# clear facility-alarm
Clearing all alarms
```

The following example shows how to clear all critical facility alarms on the router:

```
Router# clear facility-alarm critical

Clearing critical alarms
```

The following example shows how to clear minor facility alarms only:

```
Router# clear facility-alarm minor
Clearing minor alarms
```

Cisco uBR10012 Universal Broadband Router

The following example shows how to clear all alarms for both PEM modules on a Cisco uBR10012 universal broadband router:

```
Router# clear facility-alarm source pem 0
Router# clear facility-alarm source pem 1
```

Related Commands

Command	Description
facility-alarm	Sets the temperature thresholds at which the processor generates a critical, major, or minor alarm to warn of potential equipment damage.
facility-alarm critical exceed-action shutdown	Allows automatic router shutdown.
show facility-alarm	Displays the status of a generated alarm.

clear hub

To reset and reinitialize the hub hardware connected to an interface of a Cisco 2505 or Cisco 2507 router, use the **clearhub**command in user EXEC or privileged EXEC mode.

clear hub commandclear hub ethernet *number*

Syntax Description

ethernet	Hub in front of an Ethernet interface.
number	Hub number to clear, starting with 0. Because there is only one hub, this number is 0.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example clears hub 0:

```
Router#
 clear hub ethernet 0
```

Related Commands

Command	Description
hub	Enables and configures a port on an Ethernet hub of a Cisco 2505 or Cisco 2507 router.

clear hub counters

To set the hub counters on an interface of a Cisco 2505 or Cisco 2507 router to zero, use the **clearhubcounters** command in user EXEC or privileged EXEC mode.

clear hub counters commandclear hub counters [**ether** *number* [*port* [*end-port*]]]

Syntax Description

ether	(Optional) Hub in front of an Ethernet interface.
number	(Optional) Hub number for which to clear counters. Because there is currently only one hub, this number is 0. If you specify the keyword **ether**, you must specify the *number*.
port	(Optional) Port number on the hub. On the Cisco 2505 router, port numbers range from 1 to 8. On the Cisco 2507 router, port numbers range from 1 to 16. If a second port number follows, this port number indicates the end of a port range. If you do not specify a port number, counters for all ports are cleared.
end-port	(Optional) Ending port number of a range.

Command Default

If no port numbers are specified, counters for all ports are cleared.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to clear the counters displayed by a **showhub** command for all ports on hub 0:

```
Router#
 clear hub counters ether 0
```

Related Commands

Command	Description
show hub	Displays information about the hub (repeater) on an Ethernet interface of a Cisco 2505 or Cisco 2507 router.

clear interface

To reset the hardware logic on an interface, use the **clearinterface** command in user EXEC or privileged EXEC mode.

clear interface commandclear interface {*type number* [*name-tag*] | **range** *type number*}

Cisco 7200 Series and Cisco 7500 Series with a Packet OC-3 Interface Processor
clear interface {*type slot*/*port* | **range** *type number*}

Cisco 7500 Series with Ports on VIP Cards
clear interface *type slo* **t**/*port-adapter*/*port*

Cisco 7500 Series
clear interface *type slot*/*port* [**:** *channel-group*]

Cisco 7500 Series with a CT3IP Port Adapter
clear interface *type slot*/*port-adapter*/*port* [**:** *t1-channel*]

Syntax Description

type	Interface type; it is one of the keywords listed in Table 1 .
number	Port, connector, or interface card number.
name-tag	(Optional for use with the Redundant Link Manager [RLM] feature) Logic name to identify the server configuration so that multiple server configurations can be entered.
range	Clears all the interfaces within the specified range.
slot	Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information.
/ *port*	Number of the port being configured. Refer to the appropriate hardware manual for slot and port information.
port-adapter	Number of the port adapter being configured. Refer to the appropriate hardware manual for information about port adapter compatibility.
: *channel-group*	(Optional) Channel number, on Cisco 7500 series routers that support channelized T1. The range is from 0 to 23. This number is preceded by a colon.
: *t1-channel*	(Optional) For the CT3IP port adapter, the T1 channel is a number between 1 and 28. T1 channels on the CT3IP are numbered 1 to 28 rather than the more traditional zero-based scheme (0 to 27) used with other Cisco products. This numbering scheme ensures consistency with telco numbering schemes for T1 channels within channelized T3 equipment.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
11.3	This command was modified. The following changes were made: • The **vg-anylan** keyword was added • The **posi** keyword was changed to **pos**
12.0(3)T	This command was modified. The following optional argument was added for the RLM feature: • *name-tag*
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **range** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

Under normal circumstances, you do not need to clear the hardware logic on interfaces.

This command clears all the current interface hardware logic unless the type and number arguments are specified to clear only a specific interface type (serial, Ethernet, Token Ring, and so on). The table below lists the command keywords and their descriptions.

Table 6: clear interface Type Keywords

Keyword	Interface Type
acr	Virtual Automatic Call Reconnect (ACR) interface
analysis-module	Cisco network analysis service module
async	Async interface
atm	ATM interface
auto-template	Auto-Template interface
bdi	Bridge-Domain interface
bri	ISDN BRI
bvi	Bridge-Group Virtual interface
cdma-ix	CDMA Ix interface

Keyword	Interface Type
container	Container interface
ctunnel	CTunnel interface
dialer	Dialer interface
esconphy	ESCON interface
ethernet	Ethernet interface
fcpa	Fiber Channel
fddi	FDDI
filter	Filter interface
filtergroup	Filter Group interface
gigabitethernet	Gigabit Ethernet IEEE 802.3z
gmpls	MPLS interface
hssi	High-Speed Serial Interface (HSSI)
lex	Lex interface
longreachethernet	Long-Reach Ethernet interface
loopback	Loopback interface
lspvif	LSP virtual interface
mfr	Multilink Frame Relay bundle interface
multilink	Multilink-group interface
multiservice	Multiservice interface
null	Null interface
port-channel	Ethernet Channel of interfaces
portgroup	Portgroup interface
pos	Packet over SONET.
pos-channel	POS Channel of interfaces
sbc	Session Border Controller
serial	Synchronous serial interface
service-engine	Cisco service engine module
sslvpn-vif	SSLVPN Virtual Interface

Keyword	Interface Type
switch	Switch interface
sysclock	Telecom-Bus Clock Controller
tokenring	Token Ring interface
tunnel	Tunnel interface
vasileft	VasiLeft interface
vasiright	VasiRight interface
vg-anylan	100VG-AnyLAN port adapter
vif	PGM Multicast Host interface
virtual-dot11radio	Virtual dot11 interface
virtual-ppp	Virtual PPP interface
virtual-tokenring	Virtual Token Ring interface
vlan	Catalyst VLAN
vmi	Virtual Multipoint interface
voabypassin	VOA-Bypass-In interface
voabypassout	VOA-Bypass-Out interface
voafilterin	VOA-Filter-In interface
voafilterout	VOA-Filter-Out interface
voain	VOA-In interface
voaout	VOA-Out interface

Examples

The following example shows how to reset the interface logic on HSSI interface 1:

```
Router#
 clear interface hssi 1
```

The following example shows how to reset the interface logic on Packet OC-3 interface 0 on the POSIP in slot 1:

```
Router#
 clear interface pos 1/0
```

The following example shows how to reset the interface logic on T1 0 on the CT3IP port adapter in slot 9:

```
Router#
 clear interface serial 9/0/0:0
```

The following example shows how to reset the interface logic on Fast EtherChannel interface 1:

```
Router# clear interface port-channel 1
```

The following example shows how to reset demonstrates the use of the **clearinterface** command with the RLM feature:

```
Router# clear interface loopback 1
Router#
02:48:52: rlm 1: [State_Up, rx ACTIVE_LINK_BROKEN] over link [10.1.1.1(Loopback1), 10.1.4.1]
02:48:52: rlm 1: link [10.1.1.2(Loopback2), 10.1.4.2] requests activation
02:48:52: rlm 1: link [10.1.1.1(Loopback1), 10.1.4.1] is deactivated
02:48:52: rlm 1: link [10.1.1.1(Loopback1), 10.1.4.1] = socket[10.1.1.1, 10.1.4.1]
02:48:52: rlm 1: [State_Recover, rx USER_SOCKET_OPENED] over link [10.1.1.1(Loopback1),
10.1.4.1] for user RLM_MGR
02:48:52: rlm 1: link [10.1.1.1(Loopback1), 10.1.4.1] is opened
02:48:52: rlm 1: link [10.1.1.1(Loopback1), 10.1.5.1] = socket[10.1.1.1, 10.1.5.1]
02:48:52: rlm 1: [State_Recover, rx USER_SOCKET_OPENED] over link [10.1.1.1(Loopback1),
10.1.5.1] for user RLM_MGR
02:48:52: rlm 1: link [10.1.1.1(Loopback1), 10.1.5.1] is opened
02:48:52: rlm 1: [State_Recover, rx START_ACK] over link [10.1.1.2(Loopback2), 10.1.4.2]
02:48:52: rlm 1: link [10.1.1.2(Loopback2), 10.1.4.2] is activated
02:48:52: rlm 1: [State_Up, rx LINK_OPENED] over link [10.1.1.1(Loopback1), 10.1.4.1]
Router# show rlm group 1 status
RLM Group 1 Status
 User/Port: RLM_MGR/3000
 Link State: Up         Last Link Status Reported: Up_Recovered
 Next tx TID: 4         Last rx TID: 0
 Server Link Group[r1-server]:
  link [10.1.1.1(Loopback1), 10.1.4.1] = socket[standby, 10.1.1.1, 10.1.4.1]
  link [10.1.1.2(Loopback2), 10.1.4.2] = socket[active, 10.1.1.2, 10.1.4.2]
 Server Link Group[r2-server]:
  link [10.1.1.1(Loopback1), 10.1.5.1] = socket[opening, 10.1.1.1, 10.1.5.1]
  link [10.1.1.2(Loopback2), 10.1.5.2] = socket[opening, 10.1.1.2, 10.1.5.2]
Router#
02:49:52: rlm 1: [State_Up, rx UP_RECOVERED_MIN_TIMEOUT]
02:49:52: rlm 1: link [10.1.1.1(Loopback1), 10.1.4.1] requests activation
02:49:52: rlm 1: [State_Switch, rx SWITCH_ACK] over link [10.1.1.1(Loopback1), 10.1.4.1]
02:49:52: rlm 1: link [10.1.1.2(Loopback2), 10.1.4.2] is deactivated
02:49:52: rlm 1: link [10.1.1.1(Loopback1), 10.1.4.1] is activated
```

Related Commands

Command	Description
interface	Defines the IP addresses of the server, configures an interface type, and enters interface configuration mode.
show rlm group	Displays the status of the RLM group.
shutdown (RLM)	Shuts down all of the links under the RLM group.

clear interface cem

T o clear the cem channel, use the **clearinterfacecem**commandin privilege exec mode.

clear interface cem *slot/subslot/port*

Syntax Description

slot	Slot number where the SIP is installed.
subslot	Subslot number of the SIP where CEOPS SPA has been installed and circuit emulation has been configured.
port	Port number of the interface on the CEOPS SPA where circuit emulation has been configured.

Command Default

No default behavior or values.

Command Modes

Privilege Exec Mode (Exec)

Command History

Release	Modification
Cisco IOS XE Release 3.3.0S	This command was introduced.

Usage Guidelines

The **clearinterfacecem**command has been introduced on Cisco ASR 1000 Series Router in Cisco IOS XE Release 3.3.0S. The **clearinterfacecem** command is used to clear the statistics information of the cem group.

Examples

The following example shows how to clear the cem channel using the clear interface cem command:

```
Router# clear interface cem
```

Related Commands

Command	Description
show interfaces cem	Displays the statistics of the cem group.

clear interface fastethernet

To reset the controller for a specified Fast Ethernet interface, use the **clearinterfacefastethernet** command in privileged EXEC mode.

Cisco 4500 and Cisco 4700 Series
clear interface fastethernet *interface-number*

Cisco 7200 and Cisco 7500 Series
clear interface fastethernet *slot* / *port*

Cisco 7500 Series with a VIP
clear interface fastethernet *slot* / *port-adapter* / *port*

Syntax Description

interface-number	Port, connector, or interface card number. On a Cisco 4500 or Cisco 4700 Series router, specifies the number of the network processor module (NPM). The numbers are assigned at the factory at the time of installation or when added to a system.
slot	Slot number. Refer to the appropriate hardware manual for slot and port information.
/ *port*	Port number. Refer to the appropriate hardware manual for slot and port information.
/ *port-adapter*	Port adapter number. Refer to the appropriate hardware manual for information about port adapter compatibility.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

Cisco 4500 Series

The following example resets the controller for Fast Ethernet interface 0 on a Cisco 4500:

```
Router#
 clear interface fastethernet 0
```

Cisco 7200 and Cisco 7500 Series

The following example resets the controller for the Fast Ethernet interface located in slot 1, port 0 on a Cisco 7200 series router or Cisco 7500 series router:

```
Router#
 clear interface fastethernet 1/0
```

Cisco 7500 SerieswithaVIP

The following example resets the controller for the Fast Ethernet interface located in slot 1, port adapter 0, port 0 on a Cisco 7500 series router with a virtual interface processor (VIP):

```
Router#
 clear interface fastethernet 1/0/0
```

Related Commands

Command	Description
clear counters	Clears the interface counters.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show interfaces serial	Displays information about a serial interface.

clear interface gigabitethernet

To clear the hardware logic on a Gigabit Ethernet IEEE 802.3z interface, use the **clearinterfacegigabitethernet** command in privileged EXEC mode.

clear interface gigabitethernet *number*

Syntax Description

number	Gigabit Ethernet interface number; see the "Usage Guidelines" section for valid values.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The *number* argument designates the module and port number. Valid values for *number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

Examples

This example shows how to clear the hardware logic on a Gigabit Ethernet IEEE 802.3z interface:

```
Router#
clear interface gigabitethernet 5
Router#
```

Related Commands

Command	Description
show interfaces status	Displays the interface status or a list of interfaces in an error-disabled state on LAN ports only.

clear interface serial

To reset the statistical information specific to a serial interface, use the **clearinterfaceserial**command in user EXEC or privileged EXEC mode.

clear interface serial *dial-shelf/slot/t3-port* **:** *t1-num* **:** *chan-group*

Syntax Description

dial-shelf	Dial shelf chassis in the Cisco AS5800 access server that contains the CT3 interface card.
/ *slot*	Location of the CT3 interface card in the dial shelf chassis.
/ *t3-port*	T3 port number. The only valid value is 0.
: *t1-num*	T1 time slot in the T3 line. The value can be from 1 to 28.
: *chan-group*	Channel group identifier.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **clearinterfaceserial**command clears the interface hardware. To reset the counters for an interface, use the **clearcounters**command with the **serial** keyword specified. To confirm at the prompt, use the **showinterfacesserial**command.

Examples

The following example clears the interface hardware, disconnecting any active lines:

```
Router# clear interface serial 1/4/0:2:23
```

Related Commands

Command	Description
clear counters	Clears the interface counters.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show interfaces fastethernet	Displays information about a fastethernet interface.

clear interface vlan

To clear the hardware logic on a virtual local area network (VLAN), use the **clearinterfacevlan** command in privileged EXEC mode.

clear interface vlan *vlan-id*

Syntax Description

vlan-id	VLAN ID; valid values are from 1 to 4094.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on theSupervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to clear the hardware logic on a specific VLAN:

```
Router#
clear interface vlan 5
Router#
```

Related Commands

Command	Description
show interfaces status	Displays the interface status or a list of interfaces in an error-disabled state on LAN ports only.

clear ipc statistics

To clear all interprocess communication (IPC) statistics, use the **clearipcstatistics** command in privileged EXEC mode.

clear ipc statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

The **clearipcstatistics**command clears all the IPC statistics and is useful for troubleshooting issues with IPC services.

Examples

The following example shows how to clear all of the statistics used by IPC services. A **showipcstatus** command is issued first to display the current IPC counters for a local IPC server. The **clearipcstatistics** command is then entered to clear and reset the counters. A final **showipcstatus** command is issued to show that all the counters, except those counters that show the packets sent since the clearing, are reset to zero.

```
Router# show ipc status
IPC System Status
Time last IPC stat cleared : never
This processor is the IPC master server.
Do not drop output of IPC frames for test purposes.
1000 IPC Message Headers Cached.
                                                      Rx Side     Tx Side
Total Frames                                              189         140
Total from Local Ports                                    189          70
Total Protocol Control Frames                              70          44
Total Frames Dropped                                        0           0
                            Service Usage
Total via Unreliable Connection-Less Service              145           0
Total via Unreliable Sequenced Connection-Less Svc         0           0
Total via Reliable Connection-Oriented Service            44          70
                     IPC Protocol Version 0
Total Acknowledgements                                     70          44
Total Negative Acknowledgements                             0           0
                            Device Drivers
Total via Local Driver                                      0           0
Total via Platform Driver                                   0          70
Total Frames Dropped by Platform Drivers                    0           0
                    Reliable Tx Statistics
Re-Transmission                                                         0
Re-Tx Timeout                                                           0
         Rx Errors                               Tx Errors
Unsupp IPC Proto Version          0  Tx Session Error                  0
Corrupt Frame                     0  Tx Seat Error                     0
Duplicate Frame                   0  Destination Unreachable           0
Out-of-Sequence Frame             0  Tx Test Drop                      0
```

```
Dest Port does Not Exist          0  Tx Driver Failed                 0
Rx IPC Msg Alloc Failed           0  Ctrl Frm Alloc Failed            0
Unable to Deliver Msg             0
         Buffer Errors                          Misc Errors
IPC Msg Alloc                     0  IPC Open Port                    0
Emer IPC Msg Alloc                0  No HWQ                           0
IPC Frame PakType Alloc           0  Hardware Error                   0
IPC Frame MemD Alloc              0
         Tx Driver Errors
No Transport                      0
MTU Failure                       0
Dest does not Exist               0
Router# clear ipc statistics
Router# show ipc status
IPC System Status
Time last IPC stat cleared : 00:00:03
This processor is the IPC master server.
Do not drop output of IPC frames for test purposes.
1000 IPC Message Headers Cached.
                                                      Rx Side     Tx Side
Total Frames                                              26           0
Total from Local Ports                                    26           0
Total Protocol Control Frames                              0           0
Total Frames Dropped                                       0           0
Service Usage
Total via Unreliable Connection-Less Service              26           0
Total via Unreliable Sequenced Connection-Less Svc         0           0
Total via Reliable Connection-Oriented Service             0           0
IPC Protocol Version 0
Total Acknowledgements                                     0           0
Total Negative Acknowledgements                            0           0
                            Device Drivers
Total via Local Driver                                     0           0
Total via Platform Driver                                  0           0
Total Frames Dropped by Platform Drivers                   0           0
                    Reliable Tx Statistics
Re-Transmission                                                        0
Re-Tx Timeout                                                          0
         Rx Errors                              Tx Errors
Unsupp IPC Proto Version          0  Tx Session Error                 0
Corrupt Frame                     0  Tx Seat Error                    0
Duplicate Frame                   0  Destination Unreachable          0
Out-of-Sequence Frame             0  Tx Test Drop                     0
Dest Port does Not Exist          0  Tx Driver Failed                 0
Rx IPC Msg Alloc Failed           0  Ctrl Frm Alloc Failed            0
Unable to Deliver Msg             0
         Buffer Errors                          Misc Errors
IPC Msg Alloc                     0  IPC Open Port                    0
Emer IPC Msg Alloc                0  No HWQ                           0
IPC Frame PakType Alloc           0  Hardware Error                   0
IPC Frame MemD Alloc              0
         Tx Driver Errors
No Transport                      0
MTU Failure                       0
Dest does not Exist               0
```

Related Commands

Command	Description
show ipc	Displays IPC statistics.

clear lacp counters

To clear the statistics for all interfaces belonging to a specific channel group, use the **clearlacpcounters** command in privileged EXEC mode.

clear lacp [*channel-group*] **counters**

Syntax Description

channel-group	(Optional) Channel group number; valid values are from 1 to 256.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If you do not specify a *channel-group*, all channel groups are cleared.

If you enter this command for a channel group that contains members in PAgP mode, the command is ignored.

Examples

This example shows how to clear the statistics for a specific group:

```
Router# clear lacp 1 counters
Router#
```

Related Commands

Command	Description
show lacp	Displays LACP information.

clear platform netint

To clear the interrupt-throttling counters for the platform, use the **clear platform netint** command in privileged EXEC mode.

clear platform netint

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(17b)SXA	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to clear the interrupt-throttling counters for the platform:

```
Router#
clear platform netint
Router#
```

Related Commands

Command	Description
show platform netint	Displays the platform network-interrupt information.

clear platform software vnic-if-nvtable

To clear the virtual router's persistent interface database on the original VM and update the interface mapping to the hypervisor, use the **clear platform software vnic-if-nvtable** command in EXEC mode.

clear platform software vnic-if-nvtable

Command Default

No default.

Command Modes

EXEC

Command History

Release	Modification
Cisco IOS XE 3.9S	This command was introduced on the Cisco CSR 1000V.

Usage Guidelines

When the Cisco CSR 1000V boots for the first time, the vNICs on the hypervisor are mapped to the Gigabit Ethernet network interfaces on the router. The system maintains a database for mapping the interfaces, and the mapping stays persistent as long as vNICs are not removed from the system.

The **clear platform software vnic-if-nvtable** command is used when you clone the Cisco CSR 1000V configuration to a new VM. You enter the command on the cloned VM instance of the Cisco CSR 1000V so that the Gigabit Ethernet router interfaces on the cloned VM map to new vNICs. If the interface mapping from the original VM is not cleared on the cloned VM, then the Cisco CSR 1000V feature license may be invalidated.

Use the **show platform software vnic-if interface-mapping** command to verify the updated interface mapping.

Example

The following example clears the Cisco CSR 1000V interface mapping to the vNICs on the hypervisor:

```
se-10-0-0-0(config)# clear platform software vnic-if-nvtable
```

Related Commands

Command	Description
show platform software vnic-if interface-mapping	Displays the mapping between the virtual Network Interface Cards (vNICs) on the VM and the network interfaces on a virtual router.

Note Starting with the IOS XE 17.1 release, you no longer need to execute the `clear platform software vnic-int interface` command before you remove the vNIC configuration from the hypervisor. This command will be deprecated in a future release.

clear rbscp

To reset and restart a Rate Based Satellite Control Protocol (RBSCP) tunnel, use the **clearrbscp** command in privileged EXEC mode.

clear rbscp [**tunnel** *tunnel-number*]

Syntax Description

tunnel	(Optional) Resets and restarts the RBSCP tunnel interface specified in the *tunnel-number*argument. If a tunnel interface is not specified, all RBSCP tunnels are reset and restarted. • *tunnel-number* --Number of the tunnel interface in the range from 0 to 2147483647.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

The **clearrbscp**command resets the tunnel interface to its initial state and this clears RBSCP statistical information. Use this command for troubleshooting issues with RBSCP tunnels.

Examples

The following example shows how to clear the RBSCP statistics. A **showrbscpstatistics** command is issued first to display the current RBSCP counters for tunnel interface 0. The **clearrbscp**command is then entered to reset and restart tunnel interface 0. All the counters for tunnel interface 0 are reset to zero. A final **showrbscpstatistics** command is issued to show that all the counters, except those counters that show the packets sent since the clearing, are reset to zero.

```
Router# show rbscp statistics tunnel 0
Tunnel0 is up, line protocol is up
RBSCP protocol statistics:
  Init FWD-TSNs sent 15, received 11
  TUNNEL-UPs sent 10, received 5
  CLOSEDs sent 3, received 2
  TSNs sent 40, resent 2, lost by sender 1
  TSNs received 36 (duplicates 2)
  FWD-TSNs sent 144 (heartbeats 2)
  FWD-TSNs received 120 (ignored 1)
  FWD-TSNs caused 3 packet drops, 0 whole window drops
  SACKs sent 10, received 6 (ignored 1)
  Recovered with RTX 1
  Received with delay 2
  Most released at once 5
  Failed sends into the: tunnel 1, network 0
  Dropped due to: excess delay 0, tmit queue full 0
  Max on any queue: num packets: 12, num bytes: 0
  Max outstanding: 0
Router# clear rbscp tunnel 0
Tunnel0: cleared statistics
Router# show rbscp statistics tunnel 0
Tunnel0 is up, line protocol is up
RBSCP protocol statistics:
  Init FWD-TSNs sent 0, received 0
```

```
TUNNEL-UPs sent 0, received 0
CLOSEDs sent 0, received 0
TSNs sent 0, resent 0, lost by sender 0
TSNs received 0 (duplicates 0)
FWD-TSNs sent 26 (heartbeats 0)
FWD-TSNs received 0 (ignored 0)
FWD-TSNs caused 0 packet drops, 0 whole window drops
SACKs sent 0, received 0 (ignored 0)
Recovered with RTX 0
Received with delay 0
Most released at once 0
Failed sends into the: tunnel 0, network 0
Dropped due to: excess delay 0, tmit queue full 0
Max on any queue: num packets: 0, num bytes: 0
Max outstanding: 0
```

Related Commands

Command	Description
show rbscp	Displays RBSCP state and statistical information.

clear service-module serial

To reset an integrated CSU/DSU, use the **clearservice-moduleserial**command in privileged EXEC mode.

clear service-module serial *number*

Syntax Description

number	Number of the serial interface.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command only in severe circumstances (for example, when the router is not responding to a CSU/DSU configuration command).

This command terminates all DTE and line loopbacks that are locally or remotely configured. It also interrupts data transmission through the router for up to 15 seconds. The software performs an automatic software reset in case of two consecutive configuration failures.

The CSU/DSU module is not reset with the **clearinterface** command.

Caution If you experience technical difficulties with your router and intend to contact customer support, refrain from using this command. This command erases the router's past CSU/DSU performance statistics. To clear only the CSU/DSU performance statistics, issue the **clearcounters**command.

Examples

The following example show how to reset the CSU/DSU on a router:

```
Router# clear service-module serial 0
```

Related Commands

Command	Description
clear counters	Clears the interface counters.
test service-module	Performs self-tests on an integrated CSU/DSU serial interface module, such as a 4-wire, 56/64-kbps CSU/DSU.

clear top counters interface report

To clear the TopN reports, use the **cleartopcountersinterfacereport** command in privileged EXEC mode.

clear top counters interface report *number*

Syntax Description

number	(Optional) Number of ports to be displayed; valid values are from 1 to 5000 physical ports.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported on Ethernet, Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet ports only. LAN ports on the OSMs are also supported.

The **cleartopinterfacereport** command clears all the completed reports. It does not clear the pending TopN reports. When you specify a report number, the TopN task is cleared regardless of its status.

Examples

This example shows how to clear all TopN tasks:

```
Router# clear top counters interface report 1000

04:00:06: %TOPN_COUNTERS-5-DELETED: TopN report 1 deleted by the console
04:00:06: %TOPN_COUNTERS-5-DELETED: TopN report 2 deleted by the console
04:00:06: %TOPN_COUNTERS-5-DELETED: TopN report 3 deleted by the console
04:00:06: %TOPN_COUNTERS-5-DELETED: TopN report 4 deleted by the console1/24/
Router#
```

This example shows the output if you attempt to clear a pending TopN task:

```
Router# clear top counters interface report 4

04:52:12: %TOPN_COUNTERS-5-KILLED: TopN report 4 killed by the sattili onvty0 (9.10.69.9)
Router#
```

Related Commands

Command	Description
collect top counters interface	Lists the TopN processes and specific TopN reports.
show top counters interface report	Displays TopN reports and information.

clock

To configure the port clocking mode for the 1000BASE-T transceivers, use the **clock** command in interface configuration mode. To return to the default settings,use the **no** form of this command.

clock {**auto** | **active** [**prefer**] | **passive** [**prefer**]}
no clock

Syntax Description

auto	Enables the automatic-clock configuration.
active	Enables the active operation.
prefer	(Optional) Negotiates the specified mode with the far end of the link.
passive	Enables the passive operation.

Command Default

auto

Command Modes

Interface configuration

Command History

Release	Modification
12.2(17a)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported on the 1000BASE-T transceivers only.

If the clock mode of the near end of a link does not match the clock mode of the far end, the line protocol does not come up.

The active and passive clock status is determined during the auto negotiation process before the transmission link is established.

The **clock** command supports the following configurations:

- **auto** --Auto negotiates with the far end of the link but preference is given to the active-clock switch.
- **active** --Uses a local clock to determine transmitter-operation timing.
- **passive** --Recovers the clock from the received signal and uses the recovered clock to determine transmitter-operation timing.
- **active prefer** --Auto negotiates with the far end of the link but preference is given to the active-clock switch.
- **passive prefer** --Auto negotiates with the far end of the link but preference is given to the passive-clock switch.

Enter the **show running-config interface** command to display the current clock mode.

Enter the **show interfaces** command to display the clock mode that is negotiated by the firmware.

Examples

This example shows how to enable the active-clock operation:

```
Router(config-if)# clock active
Router(config-if)#
```

Related Commands

Command	Description
show interfaces	Displays traffic that is seen by a specific interface.
show running-config interface	Displays the status and configuration of the module or Layer 2 VLAN.

clock destination

To specify the IP address of a Precision Time Protocol clock destination, use the **clockdestination** command in interface configuration mode. To remove a clock destination configuration, use the **no** form of this command.

clock destination *clock-ip-address*
no clock destination *clock-ip-address*

Syntax Description

clock-ip-address	IP address of the clock destination.

Command Default

No default behavior or values.

Command Modes

Clock port configuration (config-ptp-port)

Command History

Release	Modification
15.0(1)S	This command was introduced.

Usage Guidelines

If the clock port is set to primary mode with unicast and negotiation is disabled, you can only configure a single destination. If the clock port is set to primary mode with unicast negotiation, you do not need to use this command because the device uses negotiation to determine the IP address of PTP subordinate devices.

Examples

The following example shows how to configure a PTP clock destination:

```
Device> enable
Device# configure terminal
Device(config)# ptp clock ordinary domain 0
Device(config-ptp-clk)# clock-port masterPort master
Device(config-ptp-port)# clock destination 192.168.1.2
Device(config-ptp-port)# end
```

Related Commands

Command	Description
clock source	Specifies a PTP clock source.

clock mode

To configure the clock mode of a serial circuit emulation (CEM) channel, use the **clockmode** command in CEM configuration mode. To reset the clock mode to its default, use the **no** form of this command.

clock mode {**normal** | **split**}
no clock mode

Syntax Description

normal	Specifies normal mode, in which the DCE, whether it is a CEM over IP (CEoIP) data port or the external data device, provides both the receive clock and the transmit clock to the DTE.
split	Specifies split mode, in which the DCE, whether it is a CEoIP data port or the external device, provides the receiver clock to the DTE and the DTE provides the transmit clock to the DCE.

Command Default

The serial CEM channel clock defaults to normal mode.

Command Modes

CEM configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

This command applies only to serial ports.

Examples

The following example shows how to configure the CEM clock for normal mode.

```
Router(config-cem)# clock mode normal
```

Related Commands

Command	Description
cem	Enters circuit emulation configuration mode.
clock rate	Configures the clock rate of a serial port.
clock source	Configures the clock source of a serial port.
show cem	Displays CEM statistics.

clock rate through cut-through

clock rate

To configure the clock rate for the hardware connections on serial interfaces such as network interface modules (NIMs) and interface processors to an acceptable bit rate, use the **clockrate** command in interface configuration mode. To remove the clock rate if you change the interface from a DCE to a DTE device, use the **no** form of this command. Using the **no** form of this command on a DCE interface sets the clock rate to the hardware-dependent default value.

clock rate *bps*
no clock rate

Syntax Description

bps	Desired clock rate, in bits per second: **1200**, **2400**, **4800**, **960**0, **19200**, **38400**, **56000**, **64000**, **72000**, **125000**, **148000**, **250000**, **500000**, **800000**, **1000000**, **1300000**, **2000000**, **4000000**, or **8000000** For the synchronous serial port adapters (PA-8T-V35, PA-8T-X21, PA-8T-232, and PA-4T+), a nonstandard clock rate can be used. You can enter any value from 300 to 8000000 bps. The clock rate you enter is rounded (adjusted), if necessary, to the nearest value that your hardware can support except for the following standard rates: **1200**, **2400**, **4800**, **960**0, **14400**, **19200**, **28800**, **38400**, **56000**, **64000**, **128000**, or **2015232**.

Command Default

No clock rate is configured.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
11.3	This command was modified to include nonstandard clock rates for the PA-8T-V35, PA-8T-X21, PA-8T-232, and PA-4T+ synchronous serial port adapters.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Cable Length

Be aware that the fastest speeds might not work if your cable is too long, and that speeds faster than 148,000 bits per second are too fast for EIA/TIA-232 signaling. It is recommended that you only use the synchronous serial EIA/TIA-232 signal at speeds up to 64,000 bits per second. To permit a faster speed, use EIA/TIA-449 or V.35.

Synchronous Serial Port Adapters

For the synchronous serial port adapters (PA-8T-V35, PA-8T-X21, PA-8T-232, and PA-4T+) on Cisco 7200 series routers, and on second-generation Versatile Interface Processors (VIP2s) in Cisco 7500 series routers, the clock rate you enter is rounded (if needed) to the nearest value that your hardware can support. To display the clock rate value for the port adapter, use the **showrunning-config**command.

If you plan to netboot your router over a synchronous serial port adapter interface and have a boot image prior to Cisco IOS Release 11.1(9)CA that does not support nonstandard (rounded) clock rates for the port adapters, you must use one of the following standard clock rates:

- **1200**
- **2400**
- **4800**
- **9600**
- **19200**
- **38400**
- **56000**
- **64000**

Examples

The following example shows how to set the clock rate on the first serial interface to 64,000 bps:

```
Router(config)# interface serial 0
Router(config-if)# clock rate 64000
```

The following example shows how to set the clock rate on a synchronous serial port adapter in slot 5, port 0 to 1,234,567 bps. In this example, the clock rate is adjusted to 1,151,526 bps.

```
Router(config)# interface serial 5/0
Router(config-if)# clock rate 1234567
%Clockrate rounded to nearest value that your hardware can support.
```

The following example shows how to determine the exact clock rate that the serial interface was rounded to by using the**showrunning-config** command.

```
Router# show running-config
Building configuration...
.
.
.
!
interface Serial5/0
 no ip address
 clockrate 1151526
!
.
.
.
```

clock rate (interface ATM)

To configure the clock rate between a WAN interface card (WIC) and the serial communication controllers (SCCs) that are used by the WIC, use the **clockrate** command in interface ATM configuration mode. To disable the clock rate setting, use the **no** form of this command.

clock rate [{**aal2** | **aal5**}] *clock-rate-value*
no clock rate [{**aal2** | **aal5**}] *clock-rate-value*

Syntax Description

aal2	(Optional) Specifies the ATM adaptation layer 2 (AAL2) clock rate.
aal5	(Optional) Specifies the ATM adaptation layer 5 (AAL5) clock rate.
clock-rate-value	**Clock rate value, which can be changed as follows:** • **aal2 --ForCisco1700seriesrouters,theminimumvalueforasymmetricdigitalsubscriberline(ADSL)a** **For Cisco 2600 and Cisco 3600 series routers, the minimum value for ADSL and G.SHDSL is for ADSL and G.SHDSL is 2.6 Mbps for both mainboard slots and network modules** . To make full use of the 2.3 Mbps bandwidth for Voice over ATM (VoATM) nonswitched trunk calls AAL2 clock rate as 2.6 Mbps. We recommend, however, that you keep the ADSL SCC clock rate for AAL2 at the default value of **Note** You should change the AAL2 default value on Cisco 2600 and Cisco 3600 series router for AAL2 should remain at 1 Mbps for ADSL and G.SHDSL. • **aal5** --For Cisco 1700 series routers, the minimum value for ADSL and G.SHDSL is 4 Mbps. For Cisco 2600 and Cisco 3600 series routers, the minimum value for ADSL and G.SHDSL is 1 Mb G.SHDSL is 2.6 Mbps for both mainboard slots and network modules. **Note** If you configure a clock rate that exceeds the maximum limit, the configuration will fai

Command Default

No clock rate is set

Command Modes

Interface ATM configuration

Command History

Release	Modification
12.2(8)YN	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T for the following platforms: Cisco 1721, Cisco 2610XM-2651XM, Cisco 2691, and Cisco 3660.

Usage Guidelines

The communication between digital subscriber line (DSL) WICs and a host in a router occurs through a device called the SCC. If a host wants to forward data or send any control traffic to a DSL WIC, it uses SCCs. In the same way, if a DSL WIC wants to forward incoming data from a line to the host, it also uses SCCs. Each DSL WIC installed in the router uses two SCCs. One SCC (SCC-A) is used for AAL5 data traffic, and the other SCC (SCC-B) is used for AAL2 and control traffic. The speed at which the SCC transfers data between a host and a WIC depends on the clock rate with which it has been configured. You can configure this clock rate on the basis of the DSL line rate. Even though the DSL upstream and downstream line rate may vary, the clock rate between the SCC and the DSL WIC is the same for both the transmitting and receiving direction. That is, the communication between the SCC and the DSL WIC is synchronous. Therefore, you need to configure only one clock rate for an SCC that will be used for both transmitting and receiving between an SCC and a DSL WIC.

We always recommend that you configure the SCC clock rate slightly higher than the DSL line rate to accommodate overhead between the SCC and the DSL WIC. For an asynchronous DSL WIC (for example, ADSL), the SCC clock rate depends on either the downstream or the upstream line rate, whichever is the maximum rate. For a synchronous DSL WIC (for example, G.SHDSL), the bandwidth for upstream and downstream is the same. Therefore, the SCC clock rate configuration can be based on either the upstream or the downstream line rate.

Because the maximum line rate for G.SHDSL is 2.312 Mbps, the default SCC clock rate of 2.6 Mbps for AAL5 and 1 Mbps for AAL2 should be sufficient. However, for ADSL, the clock rate may need to be configured on the basis of the current line rate. If AAL2 is used for voice traffic, the AAL2 SCC must be configured to the appropriate clock rate: 1 Mbps for ADSL and 2.6 Mbps for G.SHDSL.

The maximum data rate between an SCC and a DSL WIC depends primarily on the maximum clock rate that the SCC can support. For example, on the Cisco 2600 series mainboard, which supports two DSL WICs, the total SCC clock rate that can be configured for both WICs is 8 Mbps. Therefore, if only one DSL WIC is present on the mainboard, AAL5 and AAL2 clock rates can be configured to 7 Mbps and 1 Mbps, respectively. If two DSL WICs are supported on the mainboard, the total of 8 Mbps should be distributed among the four SCCs.

Network module SCCs also pose similar limitations. That is, on the Cisco 2600 series, the total clock rate for all four SCCs is 8 Mbps. The maximum AAL5 clock rate that may be configured on a network module is 5.3 Mbps. On the Cisco 1700 series, the maximum configurable SCC clock rate for both AAL5 and AAL2 is 8 Mbps.

If the clock rate is not configured, the SCC is reset to the default values.

The clock rate can be configured independently for each SCC. To verify the clock rate setting, use the **showrunning-config** command.

Examples

The following example shows how to set the clock rate to 2 Mbps for AAL5 and to 1.3 Mbps for AAL2 for a Cisco 2600 or Cisco 3600 series router:

```
Router (config)# interface atm1/0
Router (config-if)# no ip address
Router (config-if)# no atm ilmi-keepalive
Router (config-if)# pvc 6/65
Router (config-if)# clock rate aal5 2000000
Router (config-if)# clock rate aal2 1300000
Router (config-if)# vbr-nrt 640 640 128
Router (config-if)# tx-ring-limit 3
```

Related Commands

Command	Description
show running-config	Displays the current configuration.

clock rate (interface serial)

To configure the clock rate for the hardware connections on serial interfaces, such as network interface modules (NIMs) and interface processors, to an acceptable bit rate, use the **clockrate** command in interface configuration mode or Circuit Emulation Module (CEM) configuration mode. To remove the clock rate if you change the interface from a DCE to a DTE device, use the **no** form of this command. Using the **no** form of this command on a DCE interface sets the clock rate to the hardware-specific default value.

clock rate {**line***rate*}
no clock rate

Syntax Description

line	Specifies that the clock source is the network. **Note** This keyword is not supported on CEM serial interfaces.
rate	Desired clock rate, in bits per second (bps): **1200**, **2400**, **4800**, **9600**, **19200**, **38400**, **56000**, **64000**, **72000**, **125000**, **148000**, **250000**, **500000**, **800000**, **1000000**, **1300000**, **2000000**, **4000000**, or **8000000** For some synchronous serial port adapters a nonstandard clock rate can be used. Refer to the hardware documentation for specific supported Lvalues. You can enter any value from 300 to 8000000 bps. The clock rate you enter is rounded (adjusted), if necessary, to the nearest value that your hardware can support except for the following standard rates: **1200**, **2400**, **4800**, **9600**, **14400**, **19200**, **28800**, **38400**, **56000**, **64000**, **128000**, or **2015232**.

Command Default

No clock rate is configured.

Command Modes

Interface configuration CEM configuration in Circuit Emulation Module (CEM)

Command History

Release	Modification
10.0	This command was introduced.
11.3	This command was modified to include nonstandard clock rates for the PA-8T-V35, PA-8T-X21, PA-8T-232, and PA-4T+ synchronous serial port adapters.
12.3(2)T	This command was modified to include the **line** keyword.
12.4(5)M	The value range for the *rate* argument was updated to support additional baud rates of 300, 600, 1792K, and 1920K bps on CEM Network Modules.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Using the **no** form of this command on a DCE interface sets the clock rate to the hardware-dependent default value.

Cable Length

Be aware that the fastest speeds might not work if your cable is too long and that speeds faster than 148,000 bits per second are too fast for EIA/TIA-232 signaling. It is recommended that you use the synchronous serial EIA/TIA-232 signal at speeds up to 64,000 bits per second only. To permit a faster speed, use EIA/TIA-449 or V.35.

Synchronous Serial Port Adapters

For the synchronous serial port adapters (PA-8T-V35, PA-8T-X21, PA-8T-232, and PA-4T+) on Cisco 7200 series routers and on second-generation Versatile Interface Processors (VIP2s) in Cisco 7500 series routers, the clock rate that you enter is rounded (if needed) to the nearest value that your hardware can support. To display the clock rate value for the port adapter, use the **showrunning-config**command.

If you plan to boot from a network (TFTP) server over a synchronous serial port adapter interface and have a boot image prior to Cisco IOS Release 11.1(9)CA that does not support nonstandard (rounded) clock rates for the port adapters, you must use one of the following standard clock rates:

1200, 2400, 4800, 9600, 19200, 38400, 56000, 64000

CEM Network Modules

The following clock rates are supported on CEM Network Modules:

200, 300, 400, 600, 800, 1200, 1800, 2400, 3200, 3600, 4800, 6400, 7200, 8000, 9600, 12000, 12800, 14400, 16000, 16800, 19200, 24000, 28800, 32000, 38400, 48000, 56000, 57600, 64000, 76800, 84000, 96000, 112000, 115200, 128000, 144000, 168000, 192000, 224000, 230400, 256000, 288000, 336000, 384000, 448000, 512000, 672000, 768000, 772000, 896000, 1024000, 1152000, 1344000, 1536000, 1544000, 1792000, 1920000, 2048000

Examples

Network as Clock Source Example

The following example shows how to set the clock rate to use the network as the clock source:

```
Router(config)# interface serial 0
Router(config-if)# clock rate line
```

Clock Rate on Synchronous Serial Port Example

The following example shows how to set the clock rate on a synchronous serial port adapter in slot 5, port 0 to 1,234,567 bps. In this example, the clock rate is adjusted to 1,151,526 bps.

```
Router(config)# interface serial 5/0
Router(config-if)# clock rate 1234567
%Clockrate rounded to nearest value that your hardware can support.
```

Clock Rate Rounded on Serial Enterface Example

The following example shows how to determine the exact clock rate that the serial interface was rounded to by using the**showrunning-config** command.

```
Router# show running-config
Building configuration...
.
```

```
.
.
!
interface Serial5/0
 no ip address
 clockrate 1151526
!
```

CEM Channel Example

This example shows the statistics for the current CEM configuration.

```
Router# show cem 4/1/0
cem info
cem 4/1/0 is up
Line state is up
Operational state is active
Near end ip address: 172.31.28.2, udp port: 15901
Far end ip address: 172.31.28.10, udp port: 15901
IP payload size: 512
IP dscp : 0x28
Idle pattern length: 8 , Idle Pattern: 0xFF
Payload compression is disabled
Data protection is disabled
Dejitter buffer size is 60 ms
Channel clock rate is 2048000 bps
Physical interface is E1 unframed
Ingress packets: 32505156, dropped: 0, overruns: 0
Egress packets: 32505158, dropped: 637, lost pkts: 0
Egress out of sequence pkts: 0
Egress overruns: 16, underruns: 244
Egress corrupt pkts rcvd: 0
30 second ingress rate 2050321 bits/sec, 500 packets/sec
30 second egress rate 2050184 bits/sec, 500 packets/sec
Tx interrupts: 32504249
Reorder queue flush: 0, visited: 0, max wait window: 0
Network jitter max: 8 ms, average: 1 ms, min: 0 ms
Adaptive clock ppm correction is 2 tracking
Event history: 0x00230058
Pkts dropped by burst limit: 0
Global stats for slot 4
************************
Egr free buf: 255
Egr host overruns: 0
Egr unknown dest count: 0
Last unknown dest ip : 0.0.0.0, port: 0
Last unknown dest src ip : 0.0.0.0, port: 0
Egr process switched: 0
Egr oos: 0
Egr unknown src count: 0, last unknown src ip: 0.0.0.0, port: 0
Ingr overruns: 0
NM cpu: 53.56 53.51 53.45 53.54
```

Related Commands

Command	Description
show running-config	Displays the current configuration.
show cem	Displays circuit emulation statistics.

clock rate network-clock

To configure the network clock rate (speed) for serial ports 0 or 1 in DCE mode, use the **clockratenetwork-clock** command in interface configuration mode. To cancel the network clock rate value, use the no form of this command.

clock rate network-clock *rate*
no clock rate network-clock *rate*

Syntax Description

rate	Network clock rate, in kbps per second. The range is from 56 to 2048. The value entered should be a multiple of the value set for the **network-clockbase-rate** command. There is no default rate.

Command Default

No clock rate is set.

Command Modes

Interface configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810 multiservice access concentrator.

Usage Guidelines

This command uses a synchronized clock on the serial port. The use of this command allows the clock on the serial port to be synchronized with the clock source of controller T1 0.

To configure the clock rate for a serial port in DTE mode, use the **clockrateline** command.

Examples

The following example shows how to configure the clock rate on serial port 1 in DCE mode:

```
Router(config)# interface serial 1
Router(config-if)# clock rate network-clock 2048
```

Related Commands

Command	Description
clock rate line	Configures the line clock rate for serial ports 0 or 1 in DTE mode.
clock source (MC3810)	Specifies the clock source of a DS1 link on the Cisco MC3810 multiservice access concentrator.
network-clock base-rate	Configures the network clock base rate for universal I/O serial ports 0 and 1 on the Cisco MC3810 multiservice concentrator.

clock recovered adaptive/differential cem

To associate the clock recovered ID to the CEM group use the clock recovered adaptive or differential **cem** command in recovered clock mode

This command is also applicable to Cisco ASR 900 Series Routers.

clock recovered *clock id* **adaptive cem** *cem group no* *port-no*

clock recovered *clock id* **differential cem** *cem group no* *port-no*

Command Default

None

Command Modes

Recovered clock mode

Command History

Release	Modification
XE 3.18SP	This command was integrated into the Cisco NCS 4200 Series
XE Everest 16.5.1	This command is introduced on the Cisco ASR 900 Series Routers.

Usage Guidelines

This command is used to associate the clock recovered ID to the CEM group.

The following example shows how to associate the clock recovered ID to the CEM group.

```
recovered-clock 0 3
 clock recovered 1 adaptive cem 0 1
```

The following example shows how to associate the clock recovered ID to the CEM group.

```
recovered-clock 0 3
 clock recovered 1 differential cem 0 1
```

Related Commands

Table 7:

Command	Description
recovered-clock	Configures an associated clock ID with the corresponding CEM circuit.

clock source

To configure the clock source of a DS1 link, enter the **clocksource** command in interface configuration, controller configuration, or ATM interface configuration mode. To restore the default **line** setting, use the **no** form of this command.

clock source {**line** | **internal** | **loop-timed**}
no clock source

Syntax Description

line	Specifies that the T1/E1 link uses the recovered clock from the line. This is the default.
internal	Specifies that the T1/E1 link uses the internal clock from the interface.
loop-timed	Specifies that the T1/E1 interface takes the clock from the Rx (line) and uses it for Tx.

Command Default

The default value is **line**.

Command Modes

Interface configuration

Controller configuration for the Cisco MC3810 multiservice access concentrator.

ATM interface configuration for the Cisco 2600 and 3600 series routers.

Command History

Release	Modification
10.3	This command was introduced.
11.1 CA	This command was modified to support the E1-G.703/G.704 serial port adapter, PA-E3 serial port adapters, and Cisco 7200 series routers.
11.3 MA	This command was introduced as a controller configuration command for the Cisco MC3810.
12.0(5)T and 12.0(5)XK	The command was introduced as an ATM interface configuration command for the Cisco 2600 and 3600 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command sets clocking for individual T1/E1 links.

Make sure that you specify the clock source correctly for each link, even if you are planning to specify that a certain link will provide clocking for all the links in an IMA group. Because links may be taken in and out of service, requiring that the system select another link for common clocking, any link in an IMA group may provide the common clock.

If the ATM interface is part of an IMA group, you can use the **loop-timed** keyword to specify that the clock source is the same as the IMA group clock source.

Examples

On a Cisco 2600 or 3600 series router, the following example specifies an internal clock source for the link:

```
Router(config)# interface atm 0/2
Router(config-if)# clock source internal
```

Related Commands

Command	Description
ima clock-mode	Sets the transmit clock mode for an ATM IMA group.

clock source(10GE)

To specify the clock source of a 10 Gigabit Ethernet (GE) line card, use the **clocksource** command in interface configuration mode. To restore the clock source to its default setting, use the **no** form of this command.

clock source {**internal** | **line** | **loop**}
no clock source {**internal** | **line** | **loop**}

Syntax Description

internal	Uses the internal clock. This is the default.
line	Recovers the clock from the line.
loop	Uses local loop timing.

Command Default

The default is internal.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SRD1	This command was introduced for the 7600-ES+ITU-2TG and 7600-ES+ITU-4TG.

Usage Guidelines

When the clock source is internal, the port receive (Rx) clock is not eligible as the system clock source. The port transmit (Tx) clock is synchronized to the system clock.

When the clock source is line, the port Rx clock is eligible as the system clock source. The port Tx clock is synchronized to the system clock.

When the clock source is loop, the port Rx clock is not eligible as the system clock source. The port Tx clock is synchronized to its own Rx clock.

Examples

The following example shows how to specify line timing as the clock source:

```
Router(config)# interface TenGigabitEthernet 1/1
Router(config-if)# clock source line
```

The following example shows how to specify the internal clock on the interface provided by the 7600-ES+ITU-2TG or the 7600-ES+ITU-4TG:

```
Router(config)# interface TenGigabitEthernet 1/1
```

Router(config-if)# **clocksourceinternal**

Related Commands

Command	Description
network-clock select	Selects a source for the network clock.
show network-clocks	Displays the current configured and active network clock sources.

Command	Description
show platform hardware network-clocks	Displays network clocks for an ES+ line card.

clock source (AS5200)

To select the clock source for the time-division multiplexing (TDM) bus in a Cisco AS5200 access server, use the **clocksource** command in interface configuration mode. To restore the clock source to its default setting, use the **no** form of this command.

clock source {**line** {**primary** | **secondary**} | **internal**}
no clock source line {**primary** | **secondary**}

Syntax Description

line	Clock source on the active line.
primary	Primary TDM clock source.
secondary	Secondary TDM clock source.
internal	Selects the free running clock (also known as internal clock) as the clock source.

Command Default

The primary TDM clock source is from the T1 0 controller.

The secondary TDM clock source is from the T1 1 controller.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in 12.2S-Family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

To use the clocking coming in from a T1 line, configure the **clocksourcelineprimary** command on the T1 interface that has the most reliable clocking. Configure the **clocksourcelinesecondary** command on the T1 interface that has the next best known clocking. With this configuration, the primary line clocking is backed up to the secondary line if the primary clocking shuts down.

Examples

The following example configures the Cisco AS5200 access server to use T1 controller 0 as the primary clock source and T1 controller 1 as the secondary clock source:

```
Router(config)# controller t1 0
Router(config-controller)# clock source line primary
Router(config)# controller t1 1
Router(config-controller)# clock source line secondary
```

clock source (CEM)

To configure the clock source of a circuit emulation (CEM) network module port, use the **clocksource** command in CEM configuration mode or controller configuration mode. To return to the default clock source, use the **no** form of this command.

Cisco NM-CEM-4SER
clock source {**internal** | **loop** | **adaptive**}
no clock source {**internal** | **loop** | **adaptive**}

Cisco NM-CEM-4TE1
clock source {**internal** | **line** | **adaptive** *channel-number* [{**closed-loop** | **open-loop** | **coarse**}]}
no clock source {**internal** | **line** | **adaptive** *channel-number* [{**closed-loop** | **open-loop** | **coarse**}]}

Cisco NCS4200 Series
clock source {**internal** | **line** | **recovered**}
no clock source {**internal** | **line** | **recovered**}

Syntax Description

internal	Specifies that the clocks provided by the port to the attached CPE are derived from the router's TDM bus backplane clock (if one exists in the router) or from the onboard oscillator on the network module. This is the default clock source for a Cisco NM-CEM-4SER. For Cisco NCS 4200 Series, internal is the default clock source for channelized mode.
loop	(Cisco NM-CEM-4SER network module only) Specifies that the clock provided by the port to the attached CPE is derived from the clock received on the same port from the attached CPE.
line	(Cisco NM-CEM-4TE1 network module only) Specifies that the port transmit clock is derived from receive clock on the same port. This is the default clock source for a Cisco NM-CEM-4TE1. For Cisco NCS 4200 Series, line is the default clock source for un-channelized mode.
adaptive	Specifies that the clocks provided by the port to the attached CPE are locally synthesized on the basis of the average data content of the local dejitter buffer.
channel-number	(Cisco NM-CEM-4TE1 network module only) Number of the channel whose dejitter buffer is to be used to synthesize the transmit clock of the port.
closed-loop	(Optional; Cisco NM-CEM-4TE1 network module only) Specifies that the adaptive clock algorithm enhancements are used to improve the adaptive clock accuracy. The same clock must be used in both directions for the closed loop mode. This keyword is supported in Cisco IOS Release 12.4(2)T and later releases.
open-loop	(Optional; Cisco NM-CEM-4TE1 network module only) Specifies that some of the adaptive clock algorithm enhancements are used but the clocks do not have to be the same in both directions. This is the default. This keyword is supported in Cisco IOS Release 12.4(2)T and later releases.

coarse	(Optional; Cisco NM-CEM-4TE1 network module only) Specifies that the original adaptive clock algorithm without the enhancements is used. This keyword is supported in Cisco IOS Release 12.4(2)T and later releases.
recovered	Specifies the recovered clock number. This applies the recovered clock from a CEM interface on a T1/E1 Controller.

Command Default

The clock source defaults to **internal**.

The clock source defaults to **line**

Command Modes

CEM configuration

Controller configuration

Controller configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.4(2)T	The **closed-loop**, **open-loop**, and **coarse** keywords were added.
XE 3.18SP	This command was integrated in Cisco NCS 4200 Series.
XE Everest 16.5.1	This command was integrated in Cisco NCS 4200 Series and Cisco ASR 900 Series Routers.

Usage Guidelines

When clock source **internal** is specified, the clocks provided by the network module are derived from either of the following source:

- The router's backplane TDM clock frequency (in any router equipped with a TDM backplane bus)
- The master oscillator on the network module (in any router not equipped with a TDM backplane bus)

When the **adaptive** keyword is specified, the clocks provided by the network module are derived from the same source as in the clock source **internal** case. However, the derived frequency is further adjusted up or down on the basis of the measured average fill of the egress dejitter buffer of the connection. If the dejitter buffer is perceived to be slowly filling, the frequency is adjusted slightly upward. If the dejitter buffer is perceived to be slowly depleting, the frequency is adjusted slightly downward.

Cisco NM-CEM-4SER

When the **loop** keyword is specified, the clock provided by the NM-CEM-4SER is the same as the clock provided to the NM-CEM-4SER from the attached CPE. The specification of clock source **loop** is only valid when the **clockmodesplit** command is specified. The **clockmode** command is used only during configuration of the NM-CEM-4SER.

Cisco NM-CEM-4TE1

In Cisco IOS Release 12.4(2)T, the adaptive clocking algorithm is enhanced to provide better adaptive clock accuracy. Three new keywords are used to specify the preferred mode:

- **closed-loop** --Specifies the closed loop mode. Taking advantage of the fact that a T1 or E1 link uses the same clock in both directions, the adaptive clock algorithm enhancements are used to improve the adaptive clock accuracy. The same clock must be used in both directions for the closed loop mode, and both ends of the CEM must be running a Cisco IOS release that supports the enhanced adaptive clock algorithm. Use the closed loop mode when clock accuracy is required, the master clock from the customer premises equipment (CPE) is of good quality, and the clocks are the same in both directions of the T1 or E1 link.

Note Do not use the closed loop mode in applications where the clocks are different for the two directions of the T1 or E1 link.

- **open-loop** --Specifies the open loop mode. Some of the adaptive clock algorithm is used, but this mode does not require the clocks to be the same in both directions. This mode is compatible with previous Cisco IOS releases and is the default mode if no keyword is specified. Use the open loop mode when the master clock from the CPE is of good quality, but the clocks are not the same in both directions of the T1 or E1 link.
- **coarse** --Specifies the coarse mode. The coarse mode uses the original adaptive clock algorithm and is used when the stability of the master clock derived from the CPE is not guaranteed. This mode is compatible with previous Cisco IOS releases.

Examples

The following example shows how to configure the clock source for the serial CEM network module, NM-CEM-4SER:

```
Router(config-cem)# clock source loop
```

The following example shows how to configure the clock source for the T1/E1 CEM network module, NM-CEM-4TE1:

```
Router(config-controller)# clock source adaptive 6
```

The following example shows how to configure the clock source for an NM-CEM-4TE1 using the closed-loop mode to improve the adaptive clock accuracy:

```
Router(config-controller)# clock source adaptive 5 closed-loop
```

The following example shows how to configure the clock source for the T1 or T3 CEM network module:

```
Router(config-controller)# clock source recovered 1
```

Related Commands

Command	Description
cem	Enters circuit emulation configuration mode.
clock mode	Configures the clock mode on an NM-CEM-4SER network module.
show cem	Displays CEM channel statistics.

clock source (controller)

To set the T1 line clock source, use the **clock source** command in controller configuration mode. To restore the clock source to its default setting, use the **no** form of this command.

Cisco 4400 Integrated Services Routers

clock source [{**line** {**primary** | **secondary**} | **internal** | **network**}]

no clock source

Cisco 7200 and Cisco 7500 Series Routers

clock source [{**line** {**primary** | **secondary**} | **internal**}]

no clock source

Cisco 10000 Series Router

clock source [{**line** | **internal**}]

no clock source

Syntax Description

line	(Optional) Specifies that the interface will clock its transmitted data from a clock recovered from the line's receive data stream. This is the default.
primary	Specifies the source of primary line clocking. The default primary time-division multiplexing (TDM) clock source is from the T0 controller.
secondary	Specifies the source of secondary line clocking. The default secondary TDM clock source is from the T1 controller.
internal	(Optional) Specifies that the interface will clock its transmitted data from its internal clock.
network	(Optional) Specifies that the master clock is from the module's TDM switch. This is required for voice applications.

Command Default

Cisco 4400 Integrated Services Routers

The default clock source is line.

Cisco 7200 and Cisco 7500 Series Routers

The default clock source is line. The default primary TDM clock source is from the T0 controller. The default secondary TDM clock source is from the T1 controller. The default clock for the interface's transmitted data is from a clock recovered from the line's receive data stream from the PA-T3 serial port adapter.

Cisco 10000 Series Router

The default clock source is internal.

Command Modes

Controller configuration

Command History

Release	Modification
10.3	This command was introduced.

Release	Modification
11.1CA	This command was modified to include the T3 serial port adapter and PA-T3 serial port adapter.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.9S	This command was modified to include the **network** keyword.

Usage Guidelines

This command is available on Cisco 4000, Cisco 4400 ISR, Cisco 7000 series, Cisco 7200 series, Cisco 7500 series, and Cisco 10000 series routers. A T3 interface on a PA-T3 serial port adapter can clock its transmitted data either from its internal clock or from a clock recovered from the line's receive data stream.

Clocking on a T1 Line

To use the clocking coming in from a T1 line, configure the **clock source line primary** command on the controller that has the most reliable clocking. Configure the **clock source line secondary** command on the controller that has the next best known clocking. With this configuration, the primary line clocking is backed up to the secondary line if the primary clocking shuts down.

Cisco 10000 Series Router

The clock source cannot be specified as line on both ends of the connection.

Cisco 4400 ISR Series

The following example sets the master clock to the TDM switch:

```
Device(config)# controller t1 0/1/0
Device(config-controller)# clock source network
```

Cisco 7200

The following example shows how to configure the Cisco 7200 to use the T0 controller as the primary clocking source and the T1 controller as the secondary clocking source:

```
C7200(config)# controller t1 0
C7200(config-controller)# clock source line primary
C7200(config-controller)# exit
C7200(config)# controller t1 1
C7200(config-controller)# clock source line secondary
```

Cisco 10000 Series Router

The following example instructs the controller to use a line clock source:

```
Device(config)# controller dsx3 4/0/6
Device(config-controller)# clock source line
```

Related Commands

Command	Description
framing	Selects the frame type for the T1 or E1 data line.
linecode	Selects the line code type for T1 or E1 line.

clock source (CT3IP)

To specify where the clock source is obtained for use by the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers, use the **clocksource** command in controller configuration mode. To restore the default clock source, use the **no** form of this command.

clock source {**internal** | **line** | **loop-timed**}
no clock source

Syntax Description

internal	Specifies that the internal clock source is used. This is the default.
line	Specifies that the network clock source is used.
loop-timed	Decouples the controller clock from the system-wide clock set with the **network-clock-select** command. The loop-timed clock enables the Digital Voice Module (DVM) to connect to a PBX and to connect the Multiflex Trunk Module (MFT) to a central office when both the PBX and the central office function as DCE clock sources. This situation assumes that the PBX also takes the clocking from the central office, thereby synchronizing the clocks on the DVM and the MFT.

Command Default

The internal clock source is used.

Command Modes

Controller configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If you do not specify the **clocksource**command, the default internal clock source is used by the CT3IP.

You can also set the clock source for each T1 channel by using the **t1clocksource** controller configuration command.

Note This command replaces the **posinternal-clock** command.

Examples

The following example sets the clock source for the CT3IP to line:

```
Router(config)# controller t3 9/0/0
Router(config-controller)# clock source line
```

Related Commands

Command	Description
network-clock-select	Specifies selection priority for the clock sources.
t1 clock source	Specifies where the clock source is obtained for use by each T1 channel on the CT3IP in Cisco 7500 series routers.

clock source (interface)

To control the clock from which a G.703-E1 interface, an E1-G.703/G.704 serial port adapter, or a PA-E3 serial port adapter clocks its transmitted data, use the **clocksource** command in interface configuration mode. To restore the default clock source, use the **no** form of this command.

Cisco ASR 901 Series Aggregation Services Routers
clock source {**line** | **internal** | **loop**}
no clock source

Cisco AS5300 Access Servers
clock source {**line** {**primary** | **secondary**} | **internal**}
no clock source line {**primary** | **secondary**}

Cisco ASR 901 Series Aggregation Services Routers
clock source {**line** | **internal** | **loop**}
no clock source

Syntax Description

line	Specifies that the interface will clock its transmitted data from a clock recovered from the line's receive data stream. This is the default.
internal	Specifies that the interface will clock its transmitted data from its internal clock.
primary	Specifies the primary time-division multiplexing (TDM) clock source.
loop	Specifies that the system clock-selection process selects the clock source line as the interface. For the transmit (Tx) clock, the interface uses the clock source received on the same interface.
loop	Specifies that the system clock-selection process selects the clock source line as the interface. For the transmit (Tx) clock, the interface uses the clock source received on the same interface.

Command Default

Cisco 7000, Cisco 7200, and Cisco 7500 Series

The clock source is obtained from the receive data stream of the line.

Cisco AS5300 Access Servers

The primary TDM clock source is from the T0 controller. The secondary TDM clock source is from the T1 controller.

Cisco ASR 901 Series Aggregation Services Routers

The default clock source is internal.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced for the Cisco 4000 series, Cisco 7000 series w ith RSP7000, and Cisco 7500 series routers with the G.703 E1 interface.

Release	Modification
11.1 CA	This command was implemented on the TDM bus in a Cisco AS5200 or Cisco AS5300 access server and was modified to support the E1-G.703/G.704 serial port adapter, PA-E3 serial port adapters, and Cisco 7200 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.1(2)SNG	This command was implemented on Cisco ASR 901 Series Aggregation Services Routers. The **loop** keyword was added.
15.1(2)SNG	This command was implemented on Cisco ASR 901 Series Aggregation Services Routers. The **loop** keyword was added.

Usage Guidelines

Cisco 7000, Cisco 7200, and Cisco 7500 Series

A G.703-E1 interface , E1-G.703/G.704 serial port adapter, or a PA-E3 serial port adapter can clock its transmitted data from either its internal clock or from a clock recovered from the line’s receive data stream.

Cisco AS5300 Access Servers

To use the clocking coming in from a T1 line, configure the **clocksourcelineprimary** command on the controller that has the most reliable clocking. Configure the **clocksourcelinesecondary** command on the controller that has the next best known clocking. With this configuration, the primary line clocking is backed up to the secondary line if the primary clocking shuts down.

Examples

Cisco 7000, Cisco 7200, and Cisco 7500 Series

The following example shows how to configure the G.703-E1 interface to clock its transmitted data from its internal clock:

```
Router(config)# interface serial 0/1
Router(config-if)# clock source internal
```

Cisco ASR 901 Series Aggregation Services Routers

The following example shows how to use an internal clock source:

```
Router(config-if)# clock source internal
```

Cisco ASR 901 Series Aggregation Services Routers

The following example shows how to use an internal clock source:

```
Router(config-if)# clock source internal
```

clock source (J1 controller)

To configure the clock source for a J1 controller, use the clock source command in controller configuration mode. To restore the clock source to its default setting, use the **no** form of this command.

clock source {**line** | **internal**}
no clock source

Syntax Description

line	The controller recovers the external clock from the line and provides the recovered clock to the internal (system) clock generator. The line value is the default clock source.
internal	The controller synchronizes itself to the internal (system) clock.

Command Default

Clock source is line for the J1 controller.

Command Modes

Controller configuration

Command History

Release	Modification
11.1 T	This command was introduced.
12.2(8)T	The command was introduced as a J1 controller configuration command for the Cisco 2600 and Cisco 3600 series.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If multiple network modules are present in the router, then each J1 controller must be given a separate priority by configuration of the network-clock-select command. The controller having the highest priority will drive the internal clock.

Examples

The following example configures the clock source for line:

```
Router(config)# controller j1 3/0
Router(config-controller)# clock source line
```

Related Commands

Command	Description
network-clock-select	Sets the selection priority for a clock source.

clock source (MC3810)

To specify the clock source of a DS1 link on the Cisco MC3810 multiservice access concentrator, use the **clocksource** command in controller configuration mode. To restore the clock source to its default setting, use the **no** form of this command.

clock source {**line** | **internal** | **loop-timed**}
no clock source

Syntax Description

line	Specifies that the DS1 link uses the recovered clock. The line value is the default clock source used when the Multiflex Trunk (MFT) is installed.
internal	Specifies that the DS1 link uses the internal clock. The internal value is the default clock source used when the Digital Voice Module (DVM) is installed.
loop-timed	Specifies that the T1/E1 controller will take the clock from the Rx (line) and use it for Tx. This setting decouples the controller clock from the system-wide clock set with the **network-clock-select** command. The loop-timed clock enables the DVM to connect to a PBX and to connect the MFT to a central office when both the PBX and the central office function as DCE clock sources. This situation assumes that the PBX also takes the clocking from the central office, thereby synchronizing the clocks on the DVM and the MFT.

Command Default

Line (when the MFT is installed) Internal (when the DVM is installed)

Command Modes

Controller configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in 12.2S-Family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command applies to Voice-over-Frame Relay, Voice-over-ATM, and Voice-over-HDLC on the Cisco MC3810.

Note You cannot configure the clock source to the line setting for both T1/E1 controllers at the same time.

Examples

The following example configures the clock source for the MFT to internal, and the clock source for the DVM line on a Cisco MC3810 multiservice access concentrator:

```
Router(config)# controller T1 0
Router(config-controller)# clock source internal
Router(config)# controller T1 1
Router(config-controller)# clock source line
```

clock source (SONET controller)

To specify the clock source of a SONET controller, use the **clocksource** command in controller configuration mode. To restore the clock source to its default setting, use the **no** form of this command.

clock source {**internal** | **line** | **loop**}
no clock source

Syntax Description

internal	Specifies that the clock source uses the internal clock provided by the Route Switch Controller (RSC). This is the default.
line	Specifies that the clock source uses the primary system clock from the optical line and the recovered clock will go through the RSC phased locked loop (PLL) circuitry. Can be used when one or more STM-1 cards are installed.
loop	Specifies that the clock source uses the primary system clock from the optical line and the same recovered clock is used in the transmit (tx) direction without going through the RSC PLL circuitry. Can be used when only one STM-1 card is installed.

Command Default

Internal

Command Modes

Controller configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to specify line timing as the clock source on a SONET controller of an STM-1 card in physical slot number 2 on a Cisco AS5850:

```
Router(config)# controller sonet 2/0
Router(config-controller)# clock source line
```

clock source (T1 E1 controller)

To set clocking for individual T1 or E1 links, use the **clocksource** command in controller configuration mode. To return to the default, use the **no** form of this command.

clock source {**line** [{**primary** | **bits** | **independent**}] | **internal** [**independent**] | **free-running**}
no clock source

Syntax Description

line	Specifies that the phase-locked loop (PLL) on this controller derives its clocking from the external source to which the controller is connected, which is generally the telephone company central office (CO).
primary	(Optional) Specifies that the PLL on this controller derives its clocking from the external source to which the controller is connected. This option also puts a second port, which is generally connected to the PBX, into looped-time mode. Both ports are configured with line, but only the port connected to the external source is configured with primary.
bits	(Optional) Specifies that the controller will derive clocking from the Building Integrated Timing Supply (BITS).
independent	(Optional) Specifies that the port can operate on an independent clocking domain. Before this capability was added, on a 2-port VWIC-MFT, if both ports were configured as **clocksourceline**, the 2-port was really looped, which meant that it was getting the clock from the first port. With independent clocking mode, this dependency no longer exists, so the keyword **independent** means that both ports can be independently clocked.
internal	Specifies that the clock is generated from the T1 or E1 controller's internal PLL.
free-running	Specifies a free-running clock derived from the oscillator on the motherboard, which is used only for testing and back-to-back connections.

Command Default

The default is **line**.

Command Modes

Controller configuration

Command History

Release	Modification
12.2(2)XB	This command was introduced in controller configuration mode for Cisco 2600 series and Cisco 3660 routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(15)T	This command was implemented on the Cisco 2691 and the Cisco 3700 series.
12.3(4)XD	The **bits** keyword was added.
12.3(7)T	The **bits** keyword was integrated into Cisco IOS Release 12.3(7)T.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T and the **independent**keyword was added.

Usage Guidelines

For a detailed discussion of clock sources on individual ports, refer to "Clock Sources on Digital T1/E1 Voice Ports" in the Voice Configuration Library at the following URL: http://www.cisco.com/en/US/products/ps6441/prod_configuration_guide09186a0080565f8a.html

Examples

The following example shows the router providing clock source to two controllers:

```
Router(config)# controller E1 1/0
Router(config-controller)# framing crc
Router(config-controller)# linecoding hdb3
Router(config-controller)# clock source internal
Router(config-controller)# ds0-group timeslots 1-15 type e&m-wink-start
!
Router(config)# controller E1 1/1
Router(config-controller)# framing esf
Router(config-controller)# linecoding b8zs
Router(config-controller)# clock source internal
Router(config-controller)# ds0-group timeslots 1-15 type e&m-wink-start
```

The following example shows the digital voice hardware receiving clocking for the PLL from E1 1/0 and using this clock as a reference to clock E1 1/1. If controller E1 1/0 fails, the PLL internally generates the clock reference to drive E1 1/1.

```
Router(config)# controller E1 1/0
Router(config-controller)# framing crc
Router(config-controller)# linecoding hdb3
Router(config-controller)# clock source line
Router(config-controller)# ds0-group timeslots 1-15 type e&m-wink-start
!
Router(config)# controller E1 1/1
Router(config-controller)# framing crc4
Router(config-controller)# linecoding hdb3
Router(config-controller)# clock source internal
Router(config-controller)# ds0-group timeslots 1-15 type e&m-wink-start
```

The following example shows the router being configured to receive clocking from the BITS.

```
Router(config)# network-clock-participate slot 1
Router(config)# network-clock-select 1 E1 1/1
Router(config)# controller E1 1/1
Router(config-controller)# clock source line bits
```

Related Commands

Command	Description
controller	Configures a T1 or E1 controller and enters controller configuration mode.

clock source (T1 E1 interface)

To configure the clock source of a DS1 link, use the **clocksource** command in interface configuration or ATM interface configuration mode. To restore the default line setting, use the **no** form of this command.

clock source {**line** | **internal** | **loop-timed**}
no clock source

Syntax Description

line	Specifies that the T1/E1 link uses the recovered clock from the line. This is the default.
internal	Specifies that the T1/E1 link uses the internal clock from the interface.
loop-timed	Specifies that the T1/E1 interface takes the clock from the Rx (line) and uses it for Tx.

Command Default

line

Command Modes

Interface configuration ATM interface configuration for the Cisco 2600 and Cisco 3600 series routers

Command History

Release	Modification
10.3	This command was introduced.
11.1CA	This command was modified to support the E1-G.703/G.704 serial port adapter, PA-E3 serial port adapters, and Cisco 7200 series routers.
11.3MA	This command was introduced as a controller configuration command for the Cisco MC3810.
12.0(5)XK	The command was introduced as an ATM interface configuration command for the Cisco 2600 and Cisco 3600 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command sets clocking for individual T1/E1 links.

Make sure that you specify the clock source correctly for each link, even if you are planning to specify that a certain link will provide clocking for all the links in an IMA group. Because links may be taken in and out of service, requiring that the system select another link for common clocking, any link in an IMA group may provide the common clock.

If the ATM interface is part of an IMA group, you can use the **loop-timed** keyword to specify that the clock source is the same as the IMA group clock source.

Examples

On a Cisco 2600 or Cisco 3600 series router, the following example specifies an internal clock source for the link:

```
Router(config)# interface atm 0/2
Router(config-if)# clock source internal
```

Related Commands

Command	Description
ima clock-mode	Sets the transmit clock mode for an ATM IMA group.

clock source (T3 E3 controller)

To specify where the clock source is obtained for use by a T3 or E3 controller, use the **clocksource** command in controller configuration mode. To restore the default clock source, use the no form of this command.

clock source {**internal** | **line**}
no clock source

Syntax Description

internal	Specifies that the internal clock source is used. This is the default for T3.
line	Specifies that the network clock source is used. This is the default for E3.

Command Default

The internal clock source is used for T3 controllers. The line clock source is used for E3 controllers.

Command Modes

Controller configuration

Command History

Release	Modification
12.2(11)YT	This command was introduced on the following platforms: Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3660 series, Cisco 3725, and Cisco 3745 routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines

If you do not specify the clock source command, the default clock source is used.

Configure the **clocksourceline** command if your telephone company or the remote data service unit provides the master clock of the T3 or E3 connection.

Configure the **clocksourceinternal** command if your router provides the master clock of the T3 or E3 connection.

Note For a back-to-back connection between two T3 or E3 network modules, one controller must be configured for internal clocking while the other controller must be configured for line clocking.

Examples

The following example shows how to set the clock source to line:

```
Router(config)# controller t3 1/0
Router(config-controller)# clock source line
```

Related Commands

Command	Description
controller	Configures a T1 or E1 controller and enters controller configuration mode.

clock switchover

To specify the input lead state change that triggers the clock switching over from line to internal or from internal to line, use the clock switchover command in Data Circuit Terminating Equipment (DCE) split mode. To disable the command's effect, use the **no** form of this command.

clock switchover {**rts** | **dtr** | **ll** | **rl**} {**off** | **on**}
no clock switchover {**rts** | **dtr** | **ll** | **rl**} {**off** | **on**}

Syntax Description

off | on	On - clock switches over to internal clock when lead state is on; clock switches over to the CPE-provided clock when lead state is off. Default value. Off - clock switches over to internal clock when lead state is off; clock switches over to the CPE-provided clock when lead state is on.

Command Default

The default state is on.

Command Modes

DCE split mode (off / on).

Command History

Release	Modification
12.4(20)YA	This command was introduced.
12.4(22)T	This command is integrated into Cisco IOS Release 12.4(22)T.

Usage Guidelines

You can use the clock switchover command to switch the clock source over to internal clock. This is to provide continuity of the CEM channel when disruption of the RxC cable from the CPE occurs.

Examples

The following example shows how the clock switchover <input_lead> <off | on > command is used to check the input lead state for the clock switchover feature:

```
Router(mode-prompt
)# clock switchover <dtr> <off | on>
```

clock-port

To specify the clocking mode of a Precision Time Protocol clock port, enter clock port configuration mode using the **clock-port** command in the PTP clock configuration mode. To remove a clocking mode configuration, use the **no** form of this command.

clock-port *name* {**slave** | **master**}[{**profile g8265.1**}]
no clock-port *name* {**slave** | **master**}

Syntax Description

name	Specifies a name for the clock port.
slave	Sets the clock port to PTP subordinate mode; the port exchanges timing packets with a PTP primary device.
master	Sets the clock port to PTP primary mode; the port exchanges timing packets with PTP subordinate devices.
profile g8265.1	(Optional) Sets the clock to use the ITU-T G.8265.1 recommendations for establishing PTP sessions, determining the best primary clock, handling synchronization status message (SSM), and mapping PTP classes.

Command Default

This command is disabled by default.

Command Modes

PTP clock configuration (config-ptp-clk)

Command History

Release	Modification
15.0(1)S	This command was introduced.
15.1(2)SNG	This command was implemented on Cisco ASR 901 Series Aggregation Services Routers.
Cisco IOS Release 3.8S	The **profile g8265.1** keyword was added on Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

This command defines a new clock port and enters clock port configuration mode.

Cisco IOS XE Release 3.8S introduces support for telecom profiles, which allow you to configure a clock that uses the ITU-T G.8265.1 recommendations for establishing PTP sessions, determining the best primary clock, handling SSM, and mapping PTP classes.

Examples

The following example shows how to configure a PTP clock port:

```
Device> enable
Device# configure terminal
Device# ptp clock boundary domain 0
Device(config-ptp-clk)# clock-port slave slaveport
Device(config-ptp-port)# clock source 8.8.8.1
Device(config-ptp-port)# sync limit 1
Device(config-ptp-port)# announce timeout 4
```

```
Device(config-ptp-port)# delay-req interval 2
Device(config-ptp-port)# end
```

Related Commands

Command	Description
ptp clock	Creates a PTP clock instance.

cmt connect

To start the processes that perform the connection management (CMT) function and to allow the ring on one fiber to be started, use the **cmtconnect** command in user EXEC or privileged EXEC mode.

cmt connect [**fddi** [{*port* | *slot/port*}] [{**phy-a** | **phy-b**}]]

Syntax Description

fddi	(Optional) Identifies this as a FDDI interface.
port	(Optional) Port number . Refer to the appropriate hardware manual for slot and port information.
slot	(Optional) Slot n umber. Refer to the appropriate hardware manual for slot and port information.
phy-a	(Optional) Selects Physical Sublayer A.
phy-b	(Optional) Selects Physical Sublayer B.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

In normal operation, the FDDI interface is operational once the interface is connected and configured. The **cmtconnect** command allows the operator to start the processes that perform the CMT function.

The **cmtconnect** command is not needed in the normal operation of FDDI; this command is used mainly in interoperability tests.

This command does not have a **no** form. To stop the CMT processes, use the **cmtdisconnect** command.

Examples

The following examples demonstrate use of the **cmtconnect** command for starting the CMT processes on the FDDI ring.

The following command starts all FDDI interfaces:

```
Router# cmt connect fddi
```

The following command starts both fibers on FDDI interface unit 0:

```
Router# cmt connect fddi 0
```

The following command on the Cisco 7200 series or Cisco 7500 series starts both fibers on FDDI interface unit 0:

```
Router# cmt connect fddi 1/0
```

The following command starts only Physical Sublayer A on FDDI interface unit 0:

```
Router# cmt connect fddi 0 phy-a
```

Related Commands

Command	Description
cmt disconnect	Stops the CMT processes.

cmt disconnect

To stop the processes that perform the connection management (CMT) function and to allow the ring on one fiber to be stopped, use the **cmtdisconnect** command in user EXEC or privileged EXEC mode.

cmt disconnect [**fddi** [{*port* | *slot*/*port*}] [{**phy-a** | **phy-b**}]]

Syntax Description

fddi	(Optional) Identifies this as a FDDI interface.
port	(Optional) Port n umber. Refer to the appropriate hardware manual for slot and port information.
slot	(Optional) Slot number. Refer to the appropriate hardware manual for slot and port information.
phy-a	(Optional) Selects Physical Sublayer A.
phy-b	(Optional) Selects Physical Sublayer B.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

In normal operation, the FDDI interface is operational once the interface is connected and configured, and is turned on using the **noshutdown** command in interface configuration mode. The **cmtdisconnect** command allows the operator to stop the processes that perform the CMT function and allow the ring on one fiber to be stopped.

The **cmtdisconnect** command is not needed in the normal operation of FDDI; this command is used mainly in interoperability tests.

This command does not have a **no** form. To start the CMT processes, use the **cmtconnect** command.

Examples

The following examples demonstrate use of the **cmtdisconnect** command for stopping the CMT processes on the FDDI ring.

The following command stops all FDDI interfaces:

```
Router# cmt disconnect fddi
```

The following command stops both fibers on FDDI interface unit 0:

```
Router# cmt disconnect fddi 0
```

The following command on the Cisco 7200 series or Cisco 7500 series stops both fibers on FDDI interface unit 0:

```
Router# cmt disconnect fddi 1/0
```

The following command stops only Physical Sublayer A on the FDDI interface unit 0. This command causes the FDDI media to go into a wrapped state so that the ring will be broken.

```
Router# cmt disconnect fddi 0 phy-a
```

The following command on the Cisco 7500 series stops only Physical Sublayer A on FDDI interface unit 0 in slot 1. This command causes the FDDI media to go into a wrapped state so that the ring will be broken.

```
Router# cmt disconnect fddi 1/0 phy-a
```

Related Commands

Command	Description
cmt connect	Starts the CMT processes.

compress

To configure software compression for Link Access Procedure, Balanced (LAPB), PPP, and High-Level Data Link Control (HDLC) encapsulations, use the **compress** command in interface configuration mode. To disable compression, use the **no** form of this command.

compress {**predictor** | **stac**}
no compress {**predictor** | **stac**}

Cisco VIP2 Cards
compress {**predictor** | **stac** [{**distributed** | **software**}]}
no compress {**predictor** | **stac** [{**distributed** | **software**}]}

Cisco 7200 Series and Cisco 7500 Series
compress {**predictor** | **stac** [{**csa** *slot* | **software**}]}
no compress {**predictor** | **stac** [{**csa** *slot* | **software**}]}

PPP Encapsulation
compress [{**predictor** | **stac** | **mppc** [**ignore-pfc**]}]
no compress [{**predictor** | **stac** | **mppc** [**ignore-pfc**]}]

Syntax Description

predictor	Specifies that a predictor compression algorithm will be used on LAPB and PPP encapsulation. Compression is implemented in the software installed in the router's main processor.
stac	Specifies that a Stacker (LZS) compression algorithm will be used on LAPB, HDLC, and PPP encapsulation. For all platforms except Cisco 7200 series and platforms that support the Virtual Interface Processor 2 (VIP2), compression is implemented in the software installed in the router's main processor. On Cisco 7200 series and on VIP2s in Cisco 7500 series, specifying the **compressstac** command with no options causes the router to use the fastest available compression method for PPP encapsulation only: • If the router contains a compression service adapter (CSA), compression is performed in the CSA hardware (hardware compression). • If a CSA is not available, compression is performed in the software installed on the VIP2 (distributed compression). • If a VIP2 is not available, compression is performed in the router's main processor (software compression).
distributed	(Optional) Specifies that compression is implemented in the software that is installed in a VIP2. If the VIP2 is not available, compression is performed in the router's main processor (software compression).
software	(Optional) Specifies that compression is implemented in the Cisco IOS software installed in the router's main processor.
csa *slot*	(Optional) Specifies the CSA to use for a particular interface.

mppc	(Optional) Specifies that the Microsoft Point-to-Point Compression (MPPC) compression algorithm be used.
ignore-pfc	(Optional) Specifies that the protocol field compression flag negotiated through Link Control Protocol (LCP) will be ignored.

Command Default

Compression is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
11.3P	The following keywords were added: • **distributed** • **software** • **csa** *slot*
11.3T	The following keywords were added: • **mppc** • **ignore-pfc**
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Note This command replaces the**compresspredictor** command.

Usage Guidelines

Point-to-Point Compression

Compression reduces the size of frames through lossless data compression. You can configure point-to-point software compression for all LAPB, PPP, and HDLC encapsulations. The compression algorithm used is a predictor algorithm (the RAND compression algorithm), which uses a compression dictionary to predict what the next character in the frame will be.

End-point devices must be configured to use the same compression method (predictor, Stacker or MPPC).

HDLC encapsulations supports the Stacker compression algorithm. PPP and LAPB encapsulations support both predictor and Stacker compression algorithms.

MPPC Compression

The **compress** command using the **mppc** and **ignore-pfc** options support compression between Cisco routers and access servers and Microsoft clients, such as Windows 95 and Windows NT. MPPC implements an LZ-based compression algorithm that uses a compression dictionary to compress PPP packets. The **ignore-pfc** keyword instructs the router to ignore the protocol field compression flag negotiated by LCP. For example, the standard protocol field value for IP is 0x0021 when compression is disabled and 0x21 when compression is enabled. When the **ignore-pfc** option is enabled, the router will continue to use the uncompressed value (0x0021). Using the **ignore-pfc** option is helpful for some asynchronous driver devices that use an uncompressed protocol field (0x0021), even though the pfc is negotiated between peers. If protocol rejects are displayed when the **debugpppnegotiation** command is enabled, setting the **ignore-pfc** option may remedy the problem.

HDLC Encapsulations

For HDLC encapsulations, you can specify a Stacker compression algorithm by using the **stac** keyword. PPP and LAPB encapsulations support both predictor and Stacker compression algorithms.

Public Data Network Connections

Compression requires that both ends of the serial link be configured to use compression. You should never enable compression for connections to a public data network.

Cisco 7200 and Cisco 7500 Series

Using CSA hardware compression on Cisco 7200 series routers and Cisco 7500 series routers removes the compression and decompression responsibilities from the VIP2 or the main processor installed in the router. By using the **compressstac** command, the router determines the fastest compression method available on the router.

On Cisco 7200 series routers and Cisco 7500 series routers, hardware compression on the compression service adapter (CSA) is supported for PPP links. When using hardware compression on Cisco 7200 series routers with multiple CSAs, you can optionally specify which CSA is used by the interface to perform compression. If no CSA is specified, the router determines which CSA is used. On Cisco 7500 series routers, the router uses the CSA on the same VIP2 as the interface.

System Performance

Caution When compression is performed in software installed in the router's main processor, it might affect system performance significantly. We recommend that you disable compression if the CPU load exceeds 40 percent. To display the CPU load, use the **showprocesscpu** EXEC command.

If the majority of your traffic is already compressed files, we recommend that you not use compression. If the files are already compressed, the additional processing time spent in attempting unsuccessfully to compress them again will slow system performance.

The table below provides general guidelines for deciding which compression type to select.

Table 8: Compression Guidelines

Situation	Compression Type to Use
Bottleneck is caused by the load on the router.	Predictor
Bottleneck is the result of line bandwidth or hardware compression on the CSA is available.	Stacker
Most files are already compressed.	None

Software compression makes heavy demands on the router's processor. The maximum compressed serial line rate depends on the type of Cisco router that you are using and which compression algorithm you specify.

The table below shows a summary of the compressed serial line rates for software compression. The maximums shown in the table below apply to the “combined” serial compressed load on the router. For example, a Cisco 4000 series router could handle four 64-kbps lines using Stacker compression or one 256-kbps line. These maximums also assume that there is very little processor load on the router aside from compression. Lower these numbers when the router is required to do other processor-intensive tasks.

Table 9: Combined Compressed Serial Line Rates (Software Compression)

Compression Method	Cisco 1000 Series	Cisco 3000 Series	Cisco 4000 Series	Cisco 4500 Series	Cisco 4700 Series	Cisco 7000 Family
Stacker (kbps)	128	128	256	500	T1	256
Predictor (kbps)	256	256	500	T1	2xT1	500

Hardware compression can support a combined line rate of 16 Mbps.

Cisco recommends that you do not adjust the maximum transmission unit (MTU) for the serial interface and the LAPB maximum bits per frame (N1) parameter.

Note The best performance data compression algorithms adjust their compression methodology as they identify patterns in the data. To prevent data loss and support this adjustment process, the compression algorithm is run over LAPB to ensure that everything is sent in order, with no missing data and no duplicate data.

Note For information on configuring Frame Relay compression, refer to the “Configuring Frame Relay” chapter in the *CiscoIOSWide-AreaNetworkingConfigurationGuide*.

Examples

The following example enables hardware compression and PPP encapsulation on serial interface 3/1/0.

```
Router(config)# interface serial 3/1/0
Router(config-if)# encapsulate ppp
Router(config-if)# compress stac
```

The following example enables predictor compression on serial interface 0 for a LAPB link:

```
Router(config)# interface serial 0
Router(config-if)# encapsulation lapb
Router(config-if)# compress predictor
Router(config-if)# mtu 1509
Router(config-if)# lapb n1 12072
```

The following example enables Stacker compression on serial interface 0 for a LAPB link. This example does not set the MTU size and the maximum bits per frame (N1); we recommend that you do not change those LAPB parameters for Stacker compression:

```
Router(config)# interface serial 0
Router(config-if)# encapsulation lapb
Router(config-if)# compress predictor
```

The following example configures BRI interface 0 to perform MPPC:

```
Router(config)# interface BRI0
Router(config-if)# ip unnumbered ethernet0
Router(config-if)# encapsulation ppp
Router(config-if)# isdn spid1 5551234
Router(config-if)# dialer map ip 172.21.71.74 5551234
Router(config-if)# dialer-group 1
Router(config-if)# compress mppc
```

The following example configures asynchronous interface 1 to implement MPPC and ignore the protocol field compression flag negotiated by LCP:

```
Router(config)# interface async1
Router(config-if)# ip unnumbered ethernet0
Router(config-if)# encapsulation ppp
Router(config-if)# async default routing
Router(config-if)# async dynamic routing
Router(config-if)# async mode interactive
Router(config-if)# peer default ip address 172.21.71.74
Router(config-if)# compress mppc ignore-pfc
```

Related Commands

Command	Description
encapsulation	Sets the encapsulation method used by the interface.
encapsulation x25	Specifies operation of a serial interface as an X.25 device.
exec	Allows an EXEC process on a line.
show compress	Displays compression statistics.
show processes	Displays information about the active processes.

compress mppc

To configure compression using the Microsoft Point-to-Point Compression (MPPC) algorithm on your data compression Advanced Interface Module (AIM) for the Cisco 2600 series router, use the **compressmppc**command in interface configuration mode. To disable MPPC compression, use the **no** form of this command.

compress mppc
no compress mppc

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The MPPC compression algorithm is used to exchange compressed information with a Microsoft NT remote access server.

When configuring PPP on a serial interface, you can use hardware compression on the data compression AIM daughter card for MPPC if one is installed; otherwise you can use software compression.

Examples

The following example shows how to configure the data compression AIM daughtercard for MPPC:

```
Router(config-if)# encapsulate ppp
Router(config-if)# compress mppc
```

Related Commands

Command	Description
clear aim	Clears data compression AIM registers and resets the hardware.
compress stac caim	Specifies the exact hardware compression resource preferred.
encapsulation	Sets the encapsulation method used by the interface.
show compress	Displays compression statistics.
show pas caim	Displays debug information about the data compression AIM daughtercard.
show processes	Displays information about the active processes.

compress stac caim

To specify the hardware compression, use the **compressstaccaim**command in interface configuration mode. To disable compression, use the **no** form of this command.

compress stac caim *interface-number*
no compress stac caim *interface-number*

Syntax Description

interface-number	Interface on which compression is enabled. AIM interfaces begin with 0.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Hardware Compression

If the router contains a data compression Advanced Interface Module (CAIM), compression is performed in the CAIM hardware.

Using hardware compression in the AIM frees the main processor of the router for other tasks. You can also configure the router to use the Compression Port Module to perform compression by using the distributed option or to use the router's main processor by using the software option. If the Compression Port Module compression is performed in the main processor of the router.

Software Compression

If the CAIM is not available, compression is performed in the main processor of the router.

When compression is performed by the software installed in the router's main memory, system performance might be affected significantly. It is recommended that you disable compression in the main processor if the router CPU load exceeds 40 percent. To display the CPU load, use the show process cpu command in EXEC mode.

Examples

The following example specifies that hardware compression should be activated for CAIM interface 0:

```
Router(config-if)# encapsulation ppp
Router(config-if)# compress stac caim 0
```

Related Commands

Command	Description
clear aim	Clears data compression AIM registers and resets the hardware.
encapsulation	Sets the encapsulation method used by the interface.
show compress	Displays compression statistics.
show pas caim	Displays debug information about the data compression AIM daughtercard.
show process cpu	Displays information about the active processes on the router.

connect (module)

To create a connection between two Gigabit Ethernet (GE) enhanced network modules (ENMs) or between the GE port on an installed small-form-factor-pluggable (SFP) module and a GE ENM, or between the GE port on a switch module (SM) and another SM GE port, on a Cisco 2900 series (Cisco 2901 ISRs do not support the HIMI backplane feature.), 3800 series, or 3900 series Integrated Services Router (ISR), use the **connect** command in global configuration mode. To deactivate a connection between two GE modules on a Cisco 3800 series router, use the **no** form of this command.

connect *connection-name* **module** **module1** **channel-id1** **module** **module2** **channel-id2**
no **connect** *connection-name*

To create a dedicated connection between two GE ENMs, or between the GE port on an SFP module and a GE ENM, or between the GE port on a SM and another SM GE port, for the purpose of sending data on a specified VLAN on a Cisco 3900 series or 2900 series (Cisco 2901 ISRs do not support vlan connect in configuring the HIMI backplane feature.), use the **connect** command in global configuration mode with the **vlan***vlan-id* syntax. To deactivate a connection between two GE interfaces on a Cisco 3900 series router, 2900 series (Cisco 2901 ISRs do not support vlan connect in configuring the HIMI backplane feature.), use the **no** form of this command.

connect *connection-name* **module** **module1** **vlan** **vlan-id** **module** **module2**
no **connect** *connection-name*

Syntax Description

connection-name	Unique name for this connection.
module *module1* *channel-id1*	First of the two GE interfaces on the router between which a connection will be created. • Use the *module1* argument to identify the GE port number. Use the syntax **GigabitEthernet***slot/port* , where *slot* is the slot number in which the ENM resides, or 0 for the router onboard SFP GE port, and *port* is either the ENM port number or 0 for the router onboard SFP GE port. The following interfaces are valid: • • On the Cisco 3825 and Cisco 3845 routers, the GE port in an installed SFP module • On the Cisco 3825 router, GE interfaces in ENM slots 1 and 2 • On the Cisco 3845 router, GE interfaces in ENM slots 2 and 4 • On the Cisco 2900 (Cisco 2901 ISRs do not support the HIMI backplane feature.) series and the Cisco 3900 series routers, all interfaces and slots are permissible providing your SM and ISM supports the HIMI backplane feature. • Use the *channel-id1* argument to indicate the channel identifier on the interface slots of *module1*. On Cisco 3800 series routers, there is only one channel identifier, so this value must be 0.

module *module2* *channel-id2*	Second half of the two GE interfaces on the router between which a connection will be created. • Use the *module2* argument to identify the GE port number. Use the syntax **GigabitEthernet***slot/port* , where *slot* is the slot number in which the ENM resides, or 0 for the onboard SFP GE port, and *port* is either the ENM port number or 0 for the onboard SFP GE port. • Use the *channel-id2* argument to indicate the channel identifier on the interface slots of *module2*. On Cisco 3800 series and Cisco 3900 series routers, there is only one channel identifier, so this value must be 0.
module *module1* **vlan** vlan-id **module***module2*	Specified vlan on two GE interfaces on the router. **Note** On the Cisco 2900 series (Cisco 2901 ISRs do not support vlan connect in configuring the HIMI backplane feature.) and Cisco 3900 series routers, if your ISM or SM supports the HIMI backplane and VLAN connection, the module interconnection between the GE port (with the exception of onboard GE ports) on any slot is permitted at any given time.

Command Default

There is no connection between GE ENMs.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(2)T	This command was introduced.
15.0(1)M	This command was modified to support the Cisco 3900 series and 2900 series (Cisco 2901 ISRs do not support the HIMI backplane feature.) ISR release.

Usage Guidelines

To create a connection between two GE modules on a Cisco 2900 (Cisco 2901 ISRs do not support the HIMI backplane feature.), 3800, and 3900 series routers using the High-Speed Intrachassis Module Interconnect (HIMI) feature, use the **connect***connection-name***module** module1 channel-id1 **module** module2 channel-id2 command in global configuration mode:

Connections can be only established as follows:

- Between the GE port in an installed small-form-factor pluggable (SFP) module on the Cisco 3825 and Cisco 3845 routers
- Between GE interfaces in NME slots 1 and 2 on the Cisco 3825 router
- Between GE interfaces in NME slots 2 and 4 on the Cisco 3845 router

Note A module interconnection between the GE port on an SFP module and an ENM slot or an ENM-to-ENM cross-connection on the Cisco 3800 series routers is permitted at any time, but both types of connections cannot exist at the same time.

Note Connections between the onboard RJ-45 GE ports and ENM slots are not supported.

To create a connection between two GE SMs, to send data on a specified VLAN, on a VLAN on a Cisco 2900 (Cisco 2901 ISRs do not support the HIMI backplane feature.), and 3900, use the connect command with the with the **vlan***vlan-id* syntax.

If the **connect** command is successfully executed, the router enters connection configuration mode, which is designated by the "config-module-conn" prompt. Once the router is in connection configuration mode, the commands shown in the table below can be issued.

Table 10: Connection Configuration Mode Commands

Command	Description
default	Sets a command to its default values. Has no effect on the **connect** command functionality.
exit	Exits connection configuration mode. After you exit connection configuration mode, the actual connection establishment phase starts.
shutdown	Shuts down the connection. This command effectively deactivates the connection.
no	Negates a command or sets it to default. The **noshutdown** command reactivates a previously shut down connection.

To establish a connection, after entering connection configuration mode, issue the **exit** command to return to configuration mode. The connection will be established after you leave connection configuration mode.

Examples

The following example illustrates the creation of a connection between the onboard port GigabitEthernet0/0 and port GigabitEthernet4/0, which resides in ENM slot 4:

```
Router(config)# connect connection1 module GigabitEthernet0/0 0 module GigabitEthernet4/0
0
Router(config-module-conn)# exit
```

The following example shows the creation of a VLAN connection which is named VLAN 10 and a second VLAN connection which is named VLAN 5.

```
Router(config)# connect connection1 module gi2/0 vlan 10 module gi3/0
Router(config-module-conn)# connect connection2 module gi3/0 vlan 5 module gi4/0
Router(config-module-conn)# exit
```

Related Commands

Command	Description
show connection	Displays the status of interworking connections.

constellation

To configure the constellation for the global navigation satellite system (GNSS) module on the Cisco ASR 903, Cisco ASR 907, and the Cisco ASR 920 routers, use the **constellation** command in the gnss mode. To remove the constellation configuration, use the **no** form of this command.

constellation {**auto** | **beidou** | **galileo** | **glonass** | **gps** | **qzss**}
no constellation {**auto** | **beidou** | **galileo** | **glonass** | **gps** | **qzss**}

Syntax Description

auto	Enables auto locking to an available constellation.
beidou	Enables detection and locking to the BeiDou constellation. **Note** BeiDou and GLONAS constellations cannot be enabled simultaneously. **Note** If the `auto` option is used, BeiDou will not be part of the selected constellations.
galileo	Enables detection and locking to the Galileo constellation.
glonas	Enables detection and locking to the GLONAS constellation.
gps	Enables detection and locking to the GPS constellation.
qzss	Enables detection and locking to the QZSS constellation.

Command Default

No default behavior or values.

Command Modes

GNSS configuration (config-gnss)

Command History

Release	Modification
IOS-XE 3.17	This command was introduced on the Cisco ASR 903, Cisco ASR 907, and the Cisco ASR 920 routers.

Usage Guidelines

BeiDou and GLONAS constellations cannot be enabled simultaneously. Also, if the **auto** option is used, BeiDou will not be part of the selected constellations.

Irrespective of configured constellation, initially the GPS constellation is used for the Self-Survey mode and the GNSS module switches to using the configured constellation in over-determined mode.

Examples

The following example shows how to configure the constellations:

```
Router# configure terminal
Router(config)# gnss slot r0
Router(config-gnss)# constellation auto
```

Related Commands

Command	Description
gnss	Configures the GNSS on the router.
1pps	Configures the pulse per second from the GNSS module.
anti-jam	Enables or disables the anti-jam mode on the GNSS module.
default	Resets the device to its default state.
exit	Exists the GNSS sub mode.

control-lead sampling-rate

To configure the sampling rate of input control leads, use the **control-leadsampling-rate** command in CEM configuration mode.

control-lead sampling-rate *rate*

Syntax Description

rate	Integer that specifies the number of samples per second. Range is from 0 to 20. Default is 0.

Command Default

The input control lead sampling rate defaults to 0 (no sampling).

Command Modes

CEM configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

This command applies only to serial channels. This command does not have a **no** form; to disable control-lead sampling, set the *rate* argument to 0.

Examples

The following example shows how to configure the ingress control-lead sampling rate to 20 samples per second on a serial CEM port.

```
Router(config-cem)# control-lead sampling-rate 20
```

Related Commands

Command	Description
cem	Enters circuit emulation configuration mode.
clear cem	Clears CEM channel statistics.
control-lead state	Specifies the state of an output control lead.
show cem	Displays CEM channel statistics.

control-lead state

To specify the state of an output control lead, use the **control-leadstate** command in CEM configuration mode. The choice of output lead depends on whether the port is DCE or DTE.

control-lead state {**active** | **fail**} **output-lead** {**on** | **off** | **follow**} [{**local** | **remote**} *follow-lead*]

Syntax Description

active	Active template configuration.
fail	Failed template configuration.
output-lead	Specifies the name of the output control lead. The choice of the control lead depends on whether the port is DCE or DTE.
on	Activates the lead.
off	Deactivates the lead.
follow	Specifies the control lead state to follow.
local	(Optional) Specifies a local lead state.
remote	(Optional) Specifies a remote lead state.
follow-lead	(Optional) Specifies the local or remote input control lead for this control lead to follow. The choice of the control lead depends on whether the port is DCE or DTE.

Command Default

The default Active template that is activated depends on whether the port is DCE or DTE. The default Fail template deactivates all signals. The table below shows the various control-lead default states.

Table 11: Control-Lead Default States

Lead Number	DCE Name	DTE Name	Active Default	Fail Default
1	CTS	RTS	On	Off
2	DSR	DTR	On	Off
3	DCD	--	On	Off
4	--	LL	Off	--
5	TM	--	On	Off
6	RI	RL	Off	Off

Command Modes

CEM configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

The state of each output control lead may be specified to assume a constant level (on or off) or to change on the basis of the state of any input control lead, either at the local data port or at the remote data port.

This command applies only to serial ports. This command does not have a **no** form; to disable the control lead, specify the **off** keyword.

Examples

The following example shows how to specify the state of an output control lead.

```
Router(config-cem)# control-lead state active cts on
```

Related Commands

Command	Description
cem	Enters circuit emulation configuration mode.
control-lead sampling-rate	Configures the sampling rate of input control leads.
show cem	Displays CEM channel statistics.

controller

To configure a T1, E1, J1, or BITS controller and enter controller configuration mode, use the **controller** command in global configuration mode.

Cisco 2600 and 3600 Series Routers
controller {**t1** | **e1** | **j1**} *slot/port*

Cisco 7200 Series and Cisco 7500 Series Routers
controller {**bits** | **t1** | **e1** | **shdsl**} *slot/port/subslot-number/port-number*

Cisco AS5300 Access Servers
controller {**t1** | **e1**} *number*

Cisco ASR 901 Series Aggregation Services Routers
controller {**bits** | **t1** | **e1** | **shdsl**} *slot/port/subslot-number/port-number*

Cisco ASR 901 Series Aggregation Services Routers
controller {**bits** | **t1** | **e1** | **shdsl**} *slot/port/subslot-number/port-number*

Syntax Description

shdsl	T1 controller.
e1	E1 controller.
j1	J1 controller.
slot / port	Backplane slot number and port number on the interface. Refer to your hardware installation manual for the specific values and slot numbers.
port-number	Network processor module (NPM) number, in the range 0 through 2.
dial-shelf	Dial shelf chassis in the Cisco AS5800 access server that contains the interface card.
/ *t3-port*	T3 port number. The only valid value is 0.
port-number	Port number of the controller. Valid numbers are 0 and 1. A forward slash mark (/) is required between the slot argument and the port argument.
port-number	Port number of the controller. Valid numbers are 0 and 1. A forward slash mark (/) is required between the slot argument and the port argument.
port-number	Port number of the controller. Valid numbers are 0 and 1. A forward slash mark (/) is required between the slot argument and the port argument.
port-number	Port number of the controller. Valid numbers are 0 and 1. A forward slash mark (/) is required between the slot argument and the port argument.
port-number	Port number of the controller. Valid numbers are 0 and 1. A forward slash mark (/) is required between the slot argument and the port argument.

Command Default

No T1, E1, or J1 controller is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
10.3	The **e1** keyword was added.
12.0(3)T	Support was added for dial shelves on Cisco AS5800 access servers.
12.2(7)XO	The **j1**keyword was added for the Cisco 2600 and Cisco 3600 series.
15.1(2)SNG	This command was implemented on Cisco ASR 901 Series Aggregation Services Routers. The **bits** and **shdsl** keywords and the *subslot-number* and *port-number* arguments were added.
15.1(2)SNG	This command was implemented on Cisco ASR 901 Series Aggregation Services Routers. The **bits** and **shdsl** keywords and the *subslot-number* and *port-number* arguments were added.

Usage Guidelines

T1 or E1 Fractional Data Lines

This command is used in configurations where the router or access server is intended to communicate with a T1 or E1 fractional data line. Additional parameters for the T1 or E1 line must be configured for the controller before the T1 or E1 circuits can be configured by means of the **interface** global configuration command.

To view the status of the controllers use the **showcontrollers** command.

Examples

Cisco 7500 Series Router As a T1 Controller

The following example configures the MIP in slot 4, port 0 of a Cisco 7500 series router as a T1 controller:

```
Router(config)# controller t1 4/0
Router(config-controller)#
```

Cisco AS5800 Access Server with Dial Shelf

The following example configures the T1 controller in shelf 1, slot 0, port 0:

```
Router(config)# controller t1 1/0/0:1
Router(config-controller)#
```

Cisco 3660 As a J1 Controller

The following example configures the Cisco IOS interface card in slot 3, port 0 of a Cisco 3660 as a J1 controller:

```
Router(config)# controller j1 3/0
Router(config-controller)#
```

Related Commands

Command	Description
bert abort	Resets the T1 or E1 controller.
interface serial	Specifies a serial interface created on a channelized E1 or channelized T1 controller (for ISDN PRI, CAS, or robbed-bit signaling).
interface serial	Specifies a serial interface created on a channelized E1 or channelized T1 controller (for ISDN PRI, CAS, or robbed-bit signaling).
show controllers content-engine	Displays information about the E1 links supported by the NPM (Cisco 4000) or MIP (Cisco 7500 series).
show controllers j1	Displays information about the J1 link.
show controllers j1	Displays information about the J1 link.
show controllers t1	Displays the total number of calls and call durations on a T1 controller.

controller dsl

To configure the digital subscriber line (DSL) controller and enter controller configuration mode, use the **controllerdsl** command in global configuration mode. This command does not have a **no** form.

controller dsl *slot/port*

Syntax Description

slot	Slot number of the DSL controller. Valid numbers are 0 and 1.
/ *port*	Port number of the DSL controller. Valid numbers are 0 and 1. The slash mark (/) is required between the *slot* argument and the *port*argument.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced on Cisco 2600 series and Cisco 3700 series routers.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T on Cisco 2600 series and Cisco 3700 series routers.
12.3(11)T	This command was implemented on Cisco 2800 and Cisco 3800 series routers.
12.3(14)T	This command was implemented on Cisco 1800 series routers.

Usage Guidelines

This command is used to enter controller configuration mode for the controller in the specified slot and port. If the controller is present, it is automatically set to a default set of values, including customer premises equipment (CPE) mode and annex A.

The central office (CO) and CPE sides of the link must be configured the same in order for a connection to be made. This command is available only when the WIC-1SHDSL-V2 is installed.

Examples

The following example shows how to enter DSL controller configuration mode on the controller in slot 1 and port 0:

```
Router(config)# controller dsl
 1/0
Router(config-controller)#
```

Related Commands

Command	Description
controller shdsl	Configures the controller status.
debug xdsl application	Displays status of the xDSL if the DSL does not activate as expected.
debug xdsl driver	Displays status when the drivers are downloaded and installed.

Command	Description
debug xdsl eoc	Displays the contents of the embedded operations channel messages.
debug xdsl error	Displays the errors of xDSL process and firmware.
show controller dsl	Displays the DSL controller status and the controller number.

controller dwdm

To configure a Dense Wavelength-Division Multiplexing (DWDM) controller, use the **controllerdwdm**command in global configuration mode. This command does not have a no form.

controller dwdm *slot/port*

Syntax Description

slot/port	Number of the chassis slot that contains the interface, where: • slot--Chassis slot number. • /port--Port number.

Command Default

No default behavior or values

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRD1	This command was introduced on the Cisco 7600 series router.

Examples

The following example shows how to configure a DWDM controller in slot 3:

```
Router(config)# controller dwdm 3/1
```

Related Commands

Command	Description
g709 fec	Configures the FEC for the DWDM controller.
g709 odu threshold	Configures thresholds for selected ODU BER alarms.
g709 otu threshold	Configures thresholds for selected OTU BER alarms.
no g709 odu report	Disables the logging of selected ODU alarms.
no g709 otu report	Disables the logging of selected OTU alarms.
show controller dwdm	Displays ITU-T G.709 alarms, alerts, and counters.
show platform dwdm alarm history	Displays platform DWDM alarm history.
transport-mode	Configures a transport mode.

controller e3

To configure an E3 controller and enter controller configuration mode, use the **controllere3**command in global configuration mode.

controller e3 *slot/port*

Syntax Description

slot/port	Number of the slot and port being configured. Refer to the appropriate hardware manual for slot and port information. The slash mark is required.

Command Default

No E3 controller is configured.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(11)YT	This command was integrated into Cisco IOS Release 12.2(11)YT and implemented on the following platforms: Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3660 series, Cisco 3725, and Cisco 3745 routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
XE Everest 16.5.1	This command was integrated into Cisco ASR 900 Series Routers and Cisco NCS 4200 Series.

Examples

The following example shows the E3 controller configured in slot 0, port 0:

```
Router(config)# controller e3 0/0
Router(config-controller)#
```

Related Commands

Command	Description
controller t3	Configures a T3 controller and enters controller configuration mode.
show controllers e3	Displays information about E3 controllers.
show controllers t3	Displays information about T3 controllers.

controller mediatype

Use this command to configure MediaType controller.

mode sonet *slot* / *bay* / *port*

Syntax Description

Syntax Description:

slot	Physical slot number of the interface
bay	Bay of the interface
port	Mediatype port number

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
XE 3.18 SP	Support for this command was introduced on the NCS 4200 Series.
XE Everest 16.5.1	This command was integarted into the Cisco NCS 4200 Series and Cisco ASR 900 Series Routers.

Usage Guidelines

This command is used to configure the Mediatype controller mode. Configure the Mediatype controller mode before configuring SONET controller and T3 controller.

Examples

The following example shows how to configure Mediatype controller mode:

```
enable
configure terminal
controller MediaType 0/5/0
mode sonet
end
```

The following example shows how to set up port on the T3 interface module:

```
enable
configure terminal
controller MediaType 0/4/0
mode t3
end
```

Related Commands

Command	Description
controller sonet	Configures the SONET mode.
show controller sonet	Displays SONET controller configuration.

controller protection-group

Use this command to configure protection group controller.

controller protection-group *group id*

Syntax Description

Syntax Description:

group id	Identifier of the interface

Command Default

None

Command Modes

Controller configuration

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1	This command was introduced into the Cisco NCS 4200 Series and Cisco ASR 900 Series Routers.

Usage Guidelines

The parameters used for protection group controller are executed after using this command.

Examples

The following example shows how to configure protection group:

```
enable
configure terminal
protection-group 401 type STS48c
controller protection group 401
type STS48c
cem-group 19001 cep
end
```

Related Commands

Command	Description
show protection-group	Verifies the protection group configuration.

controller sdh

Use this command to configure a SDH controller and enter controller configuration mode.

controller sdh *slot* /*bay* /*port*

Syntax Description

Syntax Description

slot	Physical slot number. The slot is always 0 for Cisco NCS 4200 Series.
bay	Physical sub-slot or bay number. The range is 0-5.
port	SDH port number. The port number is always 0 because only one STM-1 port is supported per interface. The slash mark is required.
stm1 number	The STM number ranges from 1 to 4.

Command Default

The default port is 0.

Command Modes

Global configuration

Command History

Release	Modification
XE Everest 16.6.1	This command was integrated into the Cisco NCS 4200 Series and Cisco ASR 900 Series.

Usage Guidelines

This command does not have a **no** form because the SDH controller is created automatically when the STM-1 trunk card is detected.

Examples

```
enable
configure terminal
controller sdh 0/5/0
rate stm 4
aug mapping au-4
au-4 1
mode vc4
cem-group 100 cep
end
```

Related Commands

Command	Description
show running configuration	Verifies controller SDH configuration.

controller sonet

To configure a SONET controller and enter controller configuration mode, use the **controllersonet** command in global configuration mode.

controller sonet *slot/port*

For Cisco NCS 4200 Series

controller sonet *slot/subslot/port*

Syntax Description

bay	Identifies the bay where the VCoP SSFP is inserted. On NCS4200 series bay value is 0 always.
slot	Physical slot number. The slot number is in a range either from 0 to 5 or 8 to 13, depending on the slot in which the STM-1 card resides. The slot is always 0 for Cisco NCS 4200 Series.
/subslot	Physical sub-slot number. The range for sub-slot is 0-5.
/port	SONET port number. The port number is always 0 because only one STM-1 port is supported per interface. The slash mark is required. The range of port number for Cisco NCS 4200 Series is 8-14.

Command Default

port : 0

Command Modes

Global configuration

Command History

Release	Modification
12.0(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
XE 3.18SP	This command was integrated into Cisco NCS 4200 Series.
XE Everest 16.5.1	This command was integrated into Cisco NCS 4200 Series and Cisco ASR 920 Routers.

Usage Guidelines

This command does not have a **no** form because the SONET controller is created automatically when the STM-1 trunk card is detected by the Cisco AS5850. Use this command to specify which slot number the STM-1 card is plugged into and to configure different attributes under controller configuration mode.

Examples

The following example shows how to specify that the SONET controller is in slot number 2:

```
Router(config)# controller sonet 2/0
Router(config-controller)#
```

Examples

The following example shows how to specify that the SONET controller for Cisco NCS 4200 Series in slot number 0, sub-slot 0, and port as 8:

```
Router(config)# controller SONET 0/0/8
Router(config-controller)#
```

Related Commands

Command	Description
show controllers sonet	Displays information about SONET controllers.

controller sonet-acr

To configure a SONET Access Circuit Redundancy (ACR) virtual controller, and to enter the controller configuration mode, use the **controller sonet-acr** command in global configuration mode.

controller sonet-acr *controller unit number*

Syntax Description

controller unit number	Specifies the controller unit number. The range is 1 to 255.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
15.1(01)S	This command was introduced on the Cisco 7600 routers.

Usage Guidelines

The **controller sonet-acr**commandis used to configure channelized ATM, IMA and CEM timeslots. Before you begin the SONET ACR virtual controller configuration, ensure that you configure the APS group ACR and APS working by using the **aps group acr** *acr-group number*and **aps working** *circuit number* commandsrespectively.

Examples

This example shows how to configure the **controller sonet-acr**:

```
Router(config)# Controller sonet 4/1/0
Router(config-controller)# aps group acr 1
Router(config-controller)# aps working 1
```

The above commands on the physical controller helps in creating a virtual sonet-acr controller

```
Router(config)#
controller sonet-acr 21
```

Related Commands

Command	Description
sts-1	Configures the Synchronous Transport Signal (level)-1 in the SONET hierarchy.
vtg	Configures the (CESoPSN) CEM group.
mode vt-15	Configures the path operation mode.

controller t1/e1

To configure a T1or E1 controller and enter controller configuration mode, use the **controller** command in global configuration mode.

controller t1/**e1** *slot*/*bay*/*port*

Syntax Description

t1	Specifies T1 controller
e1	Specifies E1 controller
slot	Specifies the slot number of the interface.
bay	Specifies the bay number of the interface.
port	Specifies the port number of the interface.

Command Default

No T1 or E1controller is configured.

Command Modes

Global configuration

Command History

Release	Modification
XE 3.18SP	This command was introduced for Cisco NCS 4200 Series Routers.
XE Everest 16.5.1	This command is implemented on Cisco NCS 4200 Series and Cisco ASR 903 Series Router.

Usage Guidelines

This command is used in configurations where the router or access server is intended to communicate with a T1 or E1 fractional data line. Additional parameters for the T1 or E1 line must be configured for the controller before the T1 or E1 circuits can be configured by means of the **interface** global configuration command.

Examples

The following example shows how to configure T1 controller in slot 0, bay 1, port 1:

```
Router(config)# controller t1 0/1/1
Router(config-controller)#
```

Examples

The following example shows how to configure E1 controller in slot 0, bay 1, port 1:

```
Router(config)# controller e1 0/1/1
Router(config-controller)#
```

Related Commands

Command	Description
show controller t1/e1	Displays the total number of calls and call durations on a T1/E1 controller.

controller t3

To configure the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers or the CT3 feature board in Cisco AS5800 access servers, use the **controllert3** command in global configuration mode. To delete the defined controller, use the **no** form of this command.

Cisco 7500 Series
controller t3 *slot*/*port-adapter*/*port*
no controller t3 *slot*/*port-adapter*/*port*

Cisco AS5800 Access Server
controller t3 *dial-shelf*/*slot*/*t3-port*
no controller t3 *dial-shelf*/*slot*/*t3-port*

Cisco NCS 4200 Series
controller t3 *slot*/*sub-slot*/*port*
no controller t3 *slot*/*sub-slot*/*port*

Syntax Description

slot	Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information./
/ *port-adapter*	Number of the port adapter being configured. Refer to the appropriate hardware manual for information about port adapter compatibility.
/ *port*	Number of the port being configured. Refer to the appropriate hardware manual for slot and port information.
dial-shelf	Dial shelf chassis in the Cisco AS5800 access server containing the CT3 interface card.
/ *slot*	Location of the CT3 interface card in the dial shelf chassis.
/ *sub-slot*	Sub-slot location of the T3 interface card in the dial shelf chassis.
/ *t3-port*	T3 port number. The only valid value is 0.

Command Default

No T3 controller is configured.

No default behavior or values.

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.0(3)T	This command was implemented on the Cisco AS5800 access server.
XE 3.18SP	This command was implemented on the Cisco NCS 4200 Series.

Release	Modification
XE Everest 16.5.1	This command was implemented on the Cisco NCS 4200 Series and Cisco ASR 920 Routers.

Usage Guidelines

This command is used to configure the CT3IP and the 28 T1 channels. After the T1 channels are configured, continue to configure each T1 channel as a serial interface by using the **interfaceserial**global configuration command

Examples

Cisco 7500 Series

The following example configures the CT3IP in slot 3:

```
Router(config)# controller t3 3/0/0
```

Cisco AS5800 Access Server

The following example configures the T3 controller in shelf 3, slot 0, port 0 and T1 time slot 1:

```
Router(config)# controller t3 3/0/0
```

Cisco NCS 4200 Series

The following example configures the T3 controller in slot 0, sub-slot 4, and port 40:

```
Router(config)# controller t3 0/4/40
```

Related Commands

Command	Description
controller	Configures a T1, E1, or J1 controller and enters controller configuration mode.
interface	Specifies a serial interface created on a channelized E1 or channelized T1 controller (for ISDN PRI, CAS, or robbed-bit signaling).

copy flash lex

To download an executable image from Flash memory on the core router to a LAN Extender, use the **copyflashlex** command in privileged EXEC mode.

copy flash lex *number* **copy flash lex command**

Syntax Description

number	Number of the LAN Extender interface to which to download an image from Flash memory.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(15)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in 12.2S-Family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If you attempt to download a version of the software older than what is currently running on the LAN Extender, a warning message is displayed.

This command does not have a **no** form.

Examples

The following example copies the executable image *namexx* to LAN Extender interface 0:

```
Router# copy flash lex 0
Name of file to copy? namexx
Address of remote host [255.255.255.255] <cr>
writing namexx !!!!!!!!!!!!!!!!!!!!!!!!!copy complete
```

Related Commands

Command	Description
copy tftp lex	Downloads an executable image from a TFTP server to a LAN Extender.

copy tftp lex

To download an executable image from a TFTP server to the LAN Extender, use the **copytftplex** command privileged EXEC mode.

copy tftp lex *number* **copy tftp lex command**

Syntax Description

number	Number of the LAN Extender interface to which to download an image.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(15)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in 12.2S-Family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If you attempt to download a version of the software older than what is currently running on the LAN Extender, a warning message is displayed.

This command does not have a not form.

Examples

The following example copies the file *namexx* from the TFTP server:

```
Router# copy tftp lex 0
Address or name of remote host (255.255.255.255]? 10.108.1.111
Name of file to copy? namexx
OK to overwrite software version 1.0 with 1.1 ?[confirm] YLoading namexx from
10.108.13.111!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 127825/131072 bytes]
Successful download to LAN Extender
```

crc

To set the length of the cyclic redundancy check (CRC), use the**crc** command in interface configuration mode. To set the CRC length to the default value, use the **no** form of this command.

crc commandcrc *size-in-bits*
no crc

Syntax Description

size-in-bits	CRC size in bits. Valid values are 16 and 32. The default is 16.

Command Default

16 bits

32 bits

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

All interfaces use a 16-bit CRC by default, but also support a 32-bit CRC. CRC is an error-checking technique that uses a calculated numeric value to detect errors in transmitted data. The designators 16 and 32 indicate the length (in bits) of the frame check sequence (FCS). A CRC of 32 bits provides more powerful error detection, but adds overhead. Both the sender and receiver must use the same setting.

CRC-16, the most widely used CRC rate throughout the United States and Europe, is used extensively with WANs. CRC-32 is specified by IEEE 802 and as an option by some point-to-point transmission standards. It is often used on Switched Multimegabit Data Service (SMDS) networks and LANs.

Examples

The following example enables the 32-bit CRC on serial interface 3/0:

```
Router(config)# interface serial 3/0
Router(config-if)# crc 32
```

crc bits 5

To enable generation of CRC5 (per ITU Recommendation G.704 and G.703) to improve data integrity, use the **crcbits5**command in interface configuration mode. To disable this function, use the **no** form of this command.

crc bits 5 commandcrc bits 5
no crc bits 5

Syntax Description

This command has no arguments or keywords.

Command Default

CRC5 checking is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.1 CA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is available for the JT2 6.3-MHz serial port adapter (PA-2JT2) on the second-generation Versatile Interface Processor (VIP2), in Cisco 7500 series routers, and in Cisco 7000 series routers with the Cisco 7000 series Route Switch Processor (RSP7000) and the Cisco 7000 series Chassis Interface (RSP7000CI).

This command is useful for checking data integrity while operating in framed mode. CRC5 provides additional protection for a frame alignment signal under noisy conditions. For data transmission at JT2 (6.312 Mbps), the G.704 standard suggests 5 bits CRC. Refer to ITU Recommendation G.704 for a definition of CRC5.

You can also use the **crc** command to set the CRC size for the High-Level Data Link Control (HDLC) controllers.

Examples

The following example enables CRC5 generation on the PA-2JT2 port adapter and also sets the CRC size to 32 bits:

```
Router(config)# interface serial 0/0
Router(config-if)# crc 32
Router(config-if)# crc bits 5
```

Related Commands

Command	Description
crc	Sets the length of the CRC.

crc4

To enable generation of CRC4 (per ITU Recommendation G.704 and G.703) to improve data integrity, use the **crc4**command in interface configuration mode. To disable this function, use the **no** form of this command.

crc4
no crc4crc4 command

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
11.1 CA	This command was implemented on the Cisco 7200 series router and the E1-G.703/G.704 serial port adapter.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command applies to the Cisco 7200 series, Cisco 7000 series, and Cisco 7500 series routers. This command is supported on the Fast Serial Interface Processor (FSIP) and the E1-G.703/G.704 serial port adapter.

This command is useful for checking data integrity while operating in framed mode. CRC4 provides additional protection for a frame alignment signal under noisy conditions. For data transmission at E1 (2.048 Mbps), the G.704 standard suggests 4 bits CRC. Refer to CCITT Recommendation G.704 for a definition of CRC4.

You can also use the **crc** command to set the CRC size for the High-Level Data Link Control (HDLC) controllers.

Examples

The following example enables CRC4 generation on the E1-G.703/G.704 serial port adapter and also sets the CRC size to 32 bits:

```
Router(config)# interface serial 0/0
Router(config-if)# crc 32
Router(config-if)# crc4
```

Related Commands

Command	Description
crc	Sets the length of the CRC.

crc-threshold

To define a severely errored second (SES) by specifying the number of cyclic redundancy check (CRC) errors that occur in one second, use the **crc-threshold** command in controller configuration mode. To return to the default value, use the **no** form of this command.

crc-threshold *value*
no crc-threshold

Syntax Description

value	Number of CRC errors in one second that results in the second being declared a severely errored second (SES). Range is from 0 to 3000. Default is 320.

Command Default

A default SES is defined by a value of 320 CRC errors per second.

Command Modes

Controller configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

On a T1 port, this command applies only if extended super frame (ESF) framing is used because the super frame (SF) (also known as D4) frame structure does not include any CRC protection.

This command does not apply to an E1 port.

Examples

The following example shows how to set the CRC threshold at 512 CRC errors in one second.

```
Router(config-controller)# crc-threshold 512
```

ctunnel mode

To transport IPv4 and IPv6 packets over Connectionless Network Service (CLNS) tunnel (CTunnel), use the **ctunnelmode** command in interface configuration mode. To return the ctunnel to the default **cisco** mode, use the **no** form of this command.

ctunnel mode [{**gre** | **cisco**}]
no ctunnel mode

Syntax Description

gre	(Optional) Sets the ctunnel mode to Generic Routing Encapsulation (GRE) for transporting IPv6 packets over the CLNS network.
cisco	(Optional) Returns the ctunnel mode to the default cisco.

Command Default

Cisco encapsulation tunnel mode is the default.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

GRE tunneling of IPv4 and IPv6 packets through CLNS-only networks enables Cisco ctunnels to interoperate with networking equipment from other vendors. This feature provides compliance with RFC 3147, Generic Routing Encapsulation over CLNS Networks, which should allow interoperation between Cisco equipment and that of other vendors. in which the same standard is implemented.

RFC 3147 specifies the use of GRE when tunneling packets. The implementation of this feature does not include support for GRE header fields such as those used to specify checksums, keys, or sequencing. Any packets received which specify the use of these features will be dropped.

The default ctunnel mode continues to use the standard Cisco encapsulation. Both ends of the tunnel must be configured with the same mode for it to work. If you want to tunnel ipv6 packets you must use the new gre mode.

Examples

The following example configures a CTunnel from one router to another and shows the CTunnel destination set to 49.0001.1111.1111.1111.00. The ctunnel mode is set to gre to transport IPv6 packets.

```
interface ctunnel 301
 ipv6 address 2001:0DB8:1111:2222::2/64
```

```
ctunnel destination 49.0001.1111.1111.1111.00
ctunnel mode gre
```

Related Commands

Command	Description
clns routing	Enables routing of CLNS packets.
ctunnel destination	Specifies the destination for the CTunnel.
debug ctunnel	Displays debug messages for the IP over a CLNS Tunnel feature.
interface ctunnel	Creates a virtual interface to transport IP over a CLNS tunnel.
ip address	Sets a primary or secondary IP address for an interface.

cut-through

To configure the interfaces on the PA-12E/2FE port adapter to use cut-through switching technology between interfaces within the same bridge group, use the **cut-through**command in interface configuration mode. To return each interface to store-and-forward switching, use the **no**form of this command.

cut-through [{**receive** | **transmit**}]
no cut-through

Syntax Description

receive	(Optional) Selects cut-through switching technology on received data.
transmit	(Optional) Selects cut-through switching technology on transmitted data.

Command Default

Store-and-forward switching technology (that is, no cut-through)

Command Modes

Interface configuration

Command History

Release	Modification
11.2P	This command was introduced.’
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Cut-through mode allows switched packets to be transmitted after 64 bytes are received. The transmission of the packets can start before the end of the packet arrives. This reduces the time spent in the switch, but allows packets to be transmitted with bad cyclical redundancy checks (CRCs), because the transmission is initiated before the CRC is received or checked. Store-and-forward mode waits for the entire packet to be received before that packet is forwarded, but will check the CRC before starting transmission.

The PA-12E/2FE port adapter offloads Layer 2 switching from the host CPU by using store-and-forward or cut-through switching technology between interfaces within the same VLAN on the PA-12E/2FE port adapter. The PA-12E/2FE port adapter supports up to four VLANs (bridge groups).

Examples

The following example configures interface 3/0 for cut-through switching:

```
Router(config)#
 interface fastethernet 3/0
Router(config-if)#
 bridge-group 10
Router(config-if)#
 cut-through
Router(config-if)#
 no shutdown
Router(config-if)# exit
```

D through E

data-protection

To enable data protection for a circuit emulation (CEM) channel, use the **data-protection**command in CEM configuration mode. To disable data protection, use the **no** form of this command.

data-protection
no data-protection

Syntax Description

This command has no arguments or keywords.

Command Default

Data protection is disabled for a CEM channel.

Command Modes

CEM configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Examples

The following example demonstrates how to enable data protection.

```
Router(config-cem)# data-protection
```

Related Commands

Command	Description
cem	Enters circuit emulation configuration mode.
clear cem	Clears CEM channel statistics.
show cem	Displays CEM channel statistics.

data-strobe

To specify an input control lead to be monitored as an indicator of valid data, use the **data-strobe** command in CEM configuration mode. To disable the monitoring of an input control lead, use the **no** form of this command.

data-strobe **input-lead** {**on** | **off**}
no **data-strobe**

Syntax Description

input-lead	Specifies the input lead. The choice of leads depends on whether the port is DCE or DTE.
on	Enables packet creation when the lead is asserted.
off	Enables packet creation when the lead is deactivated.

Command Default

No input control lead is monitored.

Command Modes

CEM configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

Any input control signal on a serial data port may be configured as a "data strobe" to indicate to the NM-CEM-4SER network module whether ingress data on the port should be encapsulated for transmission or ignored. If the **data-strobe** command is specified with the **on** keyword, data packets are created and sent when the input lead is asserted. If the data strobe is off (either intentionally or as a result of the failure of the customer premises equipment [CPE]), no data packets are created, and this results in preservation of bandwidth in the IP network.

This command applies only to serial ports.

Examples

The following example demonstrates how to specify that packets are to be created and sent to the far end only when the DTR input control lead is asserted.

```
Router(config-cem)# data-strobe dtr on
```

Related Commands

Command	Description
cem	Enters circuit emulation configuration mode.
clear cem	Clears CEM channel statistics.
control-lead sampling rate	Configures the sampling rate of input control leads.
control-lead state	Specifies the state of an output control lead.
show cem	Displays CEM channel statistics.

dce-terminal-timing enable

To prevent phase shifting of the data with respect to the clock when running the line at high speeds and long distances, use the **dce-terminal-timingenable** command in interface configuration mode. If serial clock transmit external (SCTE) terminal timing is not available from the DTE, use the **no**form of this command; the DCE will use its own clock instead of SCTE from the DTE.

dce-terminal-timing enable
no dce-terminal-timing enable

Syntax Description

This command has no arguments or keywords.

Command Default

The DCE uses its own clock.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

On the Cisco 4000 router, you can specify the serial Network Interface Module timing signal configuration. When the board is operating as a DCE and the DTE provides terminal timing (SCTE or TT), the **dce-terminal-timingenable** command causes the DCE to use SCTE from the DTE.

Examples

The following example shows how to prevent phase shifting of the data with respect to the clock:

```
Router(config)# interface serial 0
Router(config-if)# dce-terminal-timing enable
```

debug l2protocol-tunnel

To configure the debugging option of Layer 2 Protocol Tunneling (L2PT), use the **debugl2protocol-tunnel** command in EXEC mode.

debug l2protocol-tunnel [{**error** | **event** | **misc** | **packet**}]

Syntax Description

error	(Optional) Displays L2PT errors.
event	(Optional) Displays L2PT events.
misc	(Optional) Displays L2PT miscellaneous.
packet	(Optional) Displays L2PT activities.

Command Default

If you do not specify a debugging option, all options are enabled.

Command Modes

User EXEC (>)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Examples

The following example shows how to debug the **l2protocol-tunnel** command:

```
Router# debug l2protocol-tunnel error
```

Related Commands

Command	Description
l2protoco-tunnel	Enables Layer 2 protocol tunneling for CDP, STP, or VTP packets on an interface.
show l2protocol-tunnel	Displays information about L2PT ports.

debug platform link-dc

To display debugging messages for the link daughter card, use the **debugplatformlink-dc**command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug platform link-dc {**dwdm** | **interface** | **interrupt** | **netclk** | **serdes** | **transceiver** | **wanphy**}
no debug platform link-dc {**dwdm** | **interface** | **interrupt** | **netclk** | **serdes** | **transceiver** | **wanphy**}

Syntax Description

dwdm	OTN G.709/DWDM driver debug information.
interface	Interface driver debug information.
interrupt	Interrupt debug information.
netclk	Network clocking debug information.
serdes	Physical layer (PHY) and SerDes debug information.
transceiver	Pluggable optics module information.
wanphy	WAN PHY driver debug information.

Command Default

Debugging is not enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRD	This command was introduced. **Note** This command applies only to the Cisco 7600 Series Ethernet Services Plus (ES+) line card on the Cisco 7600 series router.
12.2(33)SRD1	This command added the dwdm and wanphy keywords.

Usage Guidelines

Use this command with the remote command command or the attach command in privileged EXEC mode.

Examples

The following examples show the output for both the debug platform link-dc tranceiver command and the debug platform link-dc interrupt command. Notice that the show platform hardware transceiver command shows the status for the port.

```
Router# remote command module 1 debug platform link-dc tranceiver
Link-DC transceiver debugging is on
Router# remote command module 1 debug platform link-dc interrupt
Link-DC interrupt debugging is on
Router# remote command module 1 show debug
x40g subsystem:
  Link-DC transceiver debugging is on
  Link-DC interrupt debugging is on
Router# remote command module 1 show platform hardware transceiver status 1
Show status info for port 1:
```

```
TenGigabitEthernet1/1:
        State: Enabled
        Environmental Information - raw values
                Temperature: 7616
                Tx voltage: 0 in units of 100uVolt
                Tx bias: 28722 uA
                Tx power: -2 dBm (5441 in units of 0.1 uW)
                Rx power: 0 dBm (7712 in units of 0.1 uW)
                (AUX1) Laser Temperature: 8704
                (AUX2) +3.3V Supply Voltage: 32928
        XFP TX is enabled.
        XFP TX is soft enabled.
        XFP is ready.
        XFP is not power down.
        XFP is not soft power down.
        XFP doesn't have interrupt(s).
        XFP is not LOS.
        XFP data is ready.
        XFP TX path is ready.
        XFP TX laser is not in fault condition.
        XFP TX path CDR is locked.
        XFP RX path is ready.
        XFP RX path CDR is locked.
        No active alarms
        No active warning
Router-dfc1#
*Aug 15 11:20:26.436 PDT: DFC1: TenGigabitEthernet1/1 XFP: show status
*Aug 15 11:20:26.436 PDT: DFC1: TenGigabitEthernet1/1 XFP: show environmental monitoring
*Aug 15 11:20:26.436 PDT: DFC1: pluggable optics read - addr: 50, offset: 60, len: 14,
dataptr: 2377A668
*Aug 15 11:20:26.448 PDT: DFC1: pluggable optics read - addr: 50, offset: 6E, len: 2,
dataptr: 21AA028E
*Aug 15 11:20:26.452 PDT: DFC1: pluggable optics read - addr: 50, offset: 50, len: 2,
dataptr: 2377A6A0
*Aug 15 11:20:26.456 PDT: DFC1: pluggable optics read - addr: 50, offset: 52, len: 2,
dataptr: 2377A6A2
```

Note The following console log is seen when both the debug platform link-dc tranceiver command and the debug platform link-dc interrupt command are entered (as in the preceding example), and there is a transceiver Rx loss of signal (LOS) event.

```
Router-dfc1#
*Aug 15 11:23:52.127 PDT: DFC1: x40g_link_dc_interrupt_handler:  intr_status 0x8000
*Aug 15 11:23:52.127 PDT: DFC1: x40g_link_xphy_isr: xphy intr intr_st 0x80000
*Aug 15 11:23:52.127 PDT: DFC1: x40g_link_xphy_isr: xphy intr port 1
*Aug 15 11:23:52.127 PDT: DFC1: x40g_xphy_link_status_callout: port 1 link status 0
*Aug 15 11:23:52.131 PDT: DFC1: x40g_link_dc_interrupt_handler:  intr_status 0x8000
*Aug 15 11:23:52.131 PDT: DFC1: x40g_link_xphy_isr: xphy intr intr_st 0x80000
*Aug 15 11:23:52.131 PDT: DFC1: x40g_link_xphy_isr: xphy intr port 1
*Aug 15 11:23:52.131 PDT: DFC1: x40g_xphy_link_status_callout: port 1 link status 1
*Aug 15 11:23:52.135 PDT: DFC1: x40g_link_dc_process: interrupt msg_id 6, msg_num 1
*Aug 15 11:23:52.135 PDT: DFC1: x40g_link_dc_interrupt_handler:  intr_status 0x8000
*Aug 15 11:23:52.135 PDT: DFC1: x40g_link_xphy_isr: xphy intr intr_st 0x80000
*Aug 15 11:23:52.135 PDT: DFC1: x40g_link_xphy_isr: xphy intr port 1
*Aug 15 11:23:52.135 PDT: DFC1: x40g_xphy_link_status_callout: port 1 link status 0
*Aug 15 11:23:52.135 PDT: DFC1: x40g_link_dc_interrupt_handler:  intr_status 0x4000
*Aug 15 11:23:52.135 PDT: DFC1: x40g_link_xcvr_isr: intr_st 0x2, start 0, end 4, type
2,port_offset 0x0
*Aug 15 11:23:52.135 PDT: DFC1: Link xcvr port 1: Rx LOS interrupt
*Aug 15 11:23:52.135 PDT: DFC1: x40g_link_dc_process: interrupt msg_id 2, msg_num 1
```

```
*Aug 15 11:23:52.135 PDT: DFC1: Port 2: transceiver Rx LOS event
*Aug 15 11:23:52.147 PDT: DFC1: x40g_link_dc_process: xcvr oir timer timeout
00:12:37: %LINEPROTO-DFC1-5-UPDOWN: Line protocol on Interface TenGigabitEthernet1/2, changed
 state to down
*Aug 15 11:24:46.576 PDT: DFC1: x40g_link_dc_interrupt_handler:  intr_status 0x4000
*Aug 15 11:24:46.576 PDT: DFC1: x40g_link_xcvr_isr: intr_st 0x2, start 0, end 4, type
2,port_offset 0x0
*Aug 15 11:24:46.576 PDT: DFC1: Link xcvr port 1: Rx LOS interrupt
*Aug 15 11:24:46.576 PDT: DFC1: x40g_link_dc_process: interrupt msg_id 2, msg_num 1
*Aug 15 11:24:46.576 PDT: DFC1: Port 2: transceiver Rx LOS recovered
*Aug 15 11:24:46.580 PDT: DFC1: x40g_link_dc_interrupt_handler:  intr_status 0x8000
*Aug 15 11:24:46.580 PDT: DFC1: x40g_link_xphy_isr: xphy intr intr_st 0x80000
*Aug 15 11:24:46.580 PDT: DFC1: x40g_link_xphy_isr: xphy intr port 1
*Aug 15 11:24:46.580 PDT: DFC1: x40g_xphy_link_status_callout: port 1 link status 0
*Aug 15 11:24:46.584 PDT: DFC1: x40g_link_dc_interrupt_handler:  intr_status 0x8000
*Aug 15 11:24:46.584 PDT: DFC1: x40g_link_xphy_isr: xphy intr intr_st 0x80000
*Aug 15 11:24:46.584 PDT: DFC1: x40g_link_xphy_isr: xphy intr port 1
*Aug 15 11:24:46.584 PDT: DFC1: x40g_xphy_link_status_callout: port 1 link status 1
*Aug 15 11:24:46.584 PDT: DFC1: x40g_link_dc_process: interrupt msg_id 6, msg_num 1
*Aug 15 11:24:46.600 PDT: DFC1: x40g_link_dc_process: xcvr oir timer timeout
00:13:31: %LINEPROTO-DFC1-5-UPDOWN: Line protocol on Interface TenGigabitEthernet1/2, changed
 state to up
```

The following example shows the output for the debug platform link-dc dwdm command.

```
Router-dfc1# debug platform link-dc dwdm
Link-DC OTN G.709/DWDM debugging is on
*Jan 28 12:10:38.784 PDT: DFC1: Port 1: OTN Alarm Query, return ptr 228E877C
los 1, oof 0, lof 0, mfas 1, lom 0
otuAis 0, otuIae 0-0, otuBdi 0, otuTim 0
oduAis 0, oduBdi 0, oduLck 0, oduOci 0, oduPtim 0
*Jan 28 12:10:38.864 PDT: DFC1: x40g_link_pemaquid_pm_tick_timer_event(1): pm_tick timer
timeout
*Jan 28 12:10:39.364 PDT: DFC1: x40g_link_pemaquid_pm_tick_timer_event(1): pm_tick timer
timeout
*Jan 28 12:10:39.840 PDT: DFC1: Port 1: OTN Alarm Query, return ptr 228E877C
los 1, oof 0, lof 0, mfas 1, lom 0
otuAis 0, otuIae 0-0, otuBdi 0, otuTim 0
oduAis 0, oduBdi 0, oduLck 0, oduOci 0, oduPtim 0
```

The following example shows the output for the debug platform link-dc wanphy command.

```
Router-dfc1# debug platform link-dc wanphy
Link-DC WAN PHY debugging is on
*Jan 28 11:59:16.184 PDT: DFC1: Port 1 WIS alarms:
     ser 0, plm_p_far 0, ais_p_far 0, lof 0, los 0
     rdi 0, ais_l 0, lcd_p 0, plm_p 0, ais_p 0, lop 0

*Jan 28 11:59:17.184 PDT: DFC1: Port 1 WIS alarms:
     ser 0, plm_p_far 0, ais_p_far 0, lof 0, los 0
     rdi 0, ais_l 0, lcd_p 0, plm_p 0, ais_p 0, lop 0
*Jan 28 11:59:17.184 PDT: DFC1: Port 1 WIS counters: b1 0, b2 0, b3 0, fe_b2 0, fe_b3 0
*Jan 28 11:59:17.184 PDT: DFC1: Port 1 WIS J1RX: 0x0000000000000089.0x302E302E302E3000
...
*Jan 28 11:59:22.288 PDT: DFC1: Port 1 WIS alarms:
     ser 0, plm_p_far 0, ais_p_far 0, lof 0, los 0
     rdi 0, ais_l 0, lcd_p 0, plm_p 0, ais_p 0, lop 0
*Jan 28 11:59:22.288 PDT: DFC1: Port 1 WIS counters: b1 0, b2 0, b3 0, fe_b2 0, fe_b3 0
*Jan 28 11:59:22.288 PDT: DFC1: Port 1 WIS J1RX: 0x0000000000000089.0x302E302E302E3000
```

Related Commands

Command	Description
show platform hardware transceiver	Displays transceiver information on a port.

debug platform network-clock

To debug issues related to the network clock, such as alarms, out-of-resource (OOR), and active-standby sources not selected correctly, use the debug platform network-clock command in the privileged EXEC mode. To disable debugging, use the **no**no form of this command. .

debug platform network-clock
no debug platform network-clock

Command Default

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.2	This command was integrated into Cisco ASR 1000 Series routers.
Cisco IOS Release 12.2(33)SRE	This command was introduced on the Cisco 7600 Series routers.

Examples

The following example shows how to debug the network clock:

```
Router(config)# debug platform network-clock
```

debug platform software ucse

To debug the Cisco UCS E-Series Server platform software and display debug messages, use the **debug platform software ucse** command in privileged EXEC mode. To disable debug, use the **no** form of this command.

debug platform software ucse {**all** | **error** | **normal**}
no debug platform software ucse {**all** | **error** | **normal**}

Syntax Description

all	Displays all platform debug messages.
error	Displays error debug messages.
normal	Displays normal debug messages.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced on the Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Router (ISR).

Usage Guidelines

After you use the **debug platform software ucse all** command, use the appropriate **ucse** command to display debug messages.

Examples

The following example shows how to display debug messages for the **ucse subslot imc password-reset** command:

```
Router# debug platform software ucse all
Router#
Router# ucse subslot 2/0 imc password-reset
 ucse2/0/0
Password reset command sent.
Router#
 IMC ACK: UCSE password reset successful for IMC
 ACK received for UCSE: Password Reset Command
```

debug snmp tunnel-mib

To enable the debugging for configuring the IP Tunnel Management Information Base (MIB) through Simple Network Management Protocol (SNMP), use the **debugsnmptunnel-mib** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug snmp tunnel-mib
no debug snmp tunnel-mib

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.
12.2(33)SB1	This command was integrated into Cisco IOS Release 12.2(33)SB1.
12.2(44)SG	This command was integrated into Cisco IOS Release 12.2(44)SG.
Cisco IOS Release XE 2.1	This command was integrated into Cisco IOS Release XE 2.1.

Usage Guidelines

Use the **debugsnmptunnel-mib** command to verify whether a tunnel is created or deleted.

Examples

The following is sample output from the **debugsnmptunnel-mib** command. The output shows that a tunnel is created through SNMP.

```
Router# debug snmp tunnel-mib
SNMP TUNNEL-MIB debugging is on
k_tunnelInetConfigEntry_get: Entering
k_tunnelInetConfigEntry_get: Exact search
tim_client_tunnel_endpoint_data_get: Entering
tim_client_tunnel_endpoint_data_get: Exact search
tim_client_tunnel_endpoint_data_get: No element found
k_tunnelInetConfigEntry_get: Client service failed
k_tunnelInetConfigEntry_test: Entering
k_tunnelInetConfigEntry_test: Completed
k_tunnelInetConfigEntry_set: Entering
tim_client_tunnel_endpoint_data_get: Entering
tim_client_tunnel_endpoint_data_get: Exact search
tim_client_tunnel_endpoint_data_get: No element found
k_tunnelInetConfigEntry_set: Calling tunnel create
tim_client_tunnel_create: Entering
tim_client_tunnel_create: Completed
```

default (CEM)

To reset channel options to their default values, use the **default**command in CEM configuration mode.

default {**data-protection** | **dejitter-buffer** | **idle-pattern** | **ip dscp** | **ip tos** | **ip precedence** | **payload-compression** | **payload-size** | **signaling**}

Syntax Description

data-protection	Resets data protection to its default value.
dejitter-buffer	Resets the dejitter buffer to its default value.
idle-pattern	Resets the idle pattern to its default value.
ip dscp	Resets the IP differentiated services code point (DSCP) field to its default value.
ip tos	Resets the IP type of service (ToS) field to its default value.
ip precedence	Resets the IP precedence field to its default value.
payload-compression	Resets payload compression to its default value.
payload-size	Resets payload size to its default value.
signaling	Resets signaling to its default value.

Command Default

The CEM channel options are set at their configured values.

Command Modes

CEM configuration

Command History

Release	Modification
12.3(7)T	This command was introduced for CEM configuration mode.

Examples

The following example demonstrates how to reset CEM channel data protection to its default value.

```
Router(config-cem)# default data-protection
```

Related Commands

Command	Description
cem	Enters circuit emulation configuration mode.
clear cem	Clears CEM channel statistics.
data-protection	Enables data protection.
dejitter-buffer	Configures the dejitter buffer size.
idle-pattern	Defines the idle pattern that the channel transmits when it goes down.
payload-compression	Enables payload compression.

Command	Description
payload-size	Configures the payload size.
show cem	Displays CEM channel statistics.
signaling	Enables CAS signaling.

default interface

To reset the configuration of an interface back to its default values, use the **default**command in global configuration mode.

default *interface-type* *interface-number*

Syntax Description

interface-type	Type of interface. The interface types that are available to be reset to their default values will vary depending on the available interface types on the networking device and the Cisco IOS release that is installed on the device. Not all possible interface types are documented here. • **async** --Reconfigures the specified async interface to its default value. • **atm** --Reconfigures the specified ATM interface to its default value. • **bvi** --Reconfigures the specified bridge-group virtual interface to its default value. • **dialer** --Reconfigures the specified dialer interface to its default value. • **ethernet** --Reconfigures the specified Ethernet interface to its default value. • **fastethernet** --Reconfigures the specified Fast Ethernet interface to its default value. • **fddi** --Reconfigures the specified FDDI interface to its default value. • **gigabitethernet** --Reconfigures the specified Gigabit Ethernet interface to its default value. • **group-async** --Reconfigures the specified group async interface to its default value. • **loopback** --Reconfigures the specified loopback interface to its default value. • **null** --Reconfigures the specified null interface to its default value. • **pos** --Reconfigures the specified Packet over SONET (POS) interface to its default value. • **serial** --Reconfigures the specified serial interface to its default value. • **tunnel** --Reconfigures the specified tunnel interface to its default value.
interface-number	Number of the interface, slot, router shelf, unit, port, or port adaptor if appropriate for the interface type. Slash marks may be required between elements of this argument.

Command Default

Existing interface configuration values are not reset.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **default** command is a general-purpose command that is not limited to interfaces; it resets defaults based on the command name that follows it. Use the **default**(interface) command when you need to remove any configuration for a specified interface and reset the interface to its default values.

Examples

The following example demonstrates how to reset serial interface 0 to its default values.

```
Router(config)# default serial 0
```

Related Commands

Commands	Description
interface	Enters interface configuration mode.

define interface-range

To create an interface-range macro, use the **define interface-range** command in global configuration mode. To remove an interface-range macro, use the **no** form of this command.

define interface-range *macro-name interface-range*

Syntax Description

macro-name	Name of the interface-range macro.
interface-range	Type of interface range. • For a list of valid values, see the "Usage Guidelines" section.

Command Default

Interface-range macro is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	This command was introduced.
12.2(17d)SXB	This command was integrated into Cisco IOS XE Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

- The **define interface-range** command applies a particular configuration on multiple interfaces and creates multiple logical, and sub interfaces.
- An interface range macro name can comprise up to 32 characters.
- An interface range for a macro can accept a maximum of five ranges. However, the subinterface range for a macro accepts only one range.
- An interface range cannot span slots.
- Use the *interface-type slot/first-interface last-interface* format to enter the interface range.
- Valid values for the *interface-type* argument are as follows:
  - **atm** —Supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2
  - **ethernet**
  - **fastethernet**
  - **ge-wan** —Supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2
  - **gigabitethernet**
  - **loopback**
  - **port-channel** *interface-number* —Valid values are from 1 to 256
  - **pos** —Supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2

- **tengigabitethernet**
- **tunnel**
- **vlan** *vlan-id* —Valid values are from 1 to 4094

Examples

The following example shows how to create a multiple-interface macro:

```
Device(config)# define interface-range macro1 ethernet 1/2 - 5, fastethernet 5/5 - 10
```

The following example shows how to create multiple loopback interfaces:

```
Device(config)# define interface-range loopback1-10
```

Related Commands

Command	Description
interface range	Executes a command on multiple ports at the same time.

dejitter-buffer

To configure the size of the dejitter buffer, use the **dejitter-buffer** command in CEM configuration mode. To restore the dejitter buffer to its default size, use the **no** form of this command.

dejitter-buffer *size*
no dejitter-buffer

Syntax Description

size	Size, in milliseconds, of the dejitter buffer. The range is from 5 to 500. The default is 60. For Cisco ASR 901 Series Aggregation Services Routers, the range is from 4 to 500; the default is 4.

Command Default

The dejitter buffer defaults to 60 milliseconds. For Cisco ASR 901 Series Aggregation Services Routers, the default is 4.

Command Modes

CEM configuration

Command History

Release	Modification
15.1(2)SNG	This command was implemented on Cisco ASR 901 Series Aggregation Services Routers.
15.1(2)SNG	This command was implemented on Cisco ASR 901 Series Aggregation Services Routers.

Examples

The following example shows how to set the dejitter buffer to 200 milliseconds.

```
Router(config-cem)# dejitter-buffer 200
```

The following example shows how to specify the size of the dejitter buffer to 10 milliseconds on the Cisco ASR 901 Series Aggregation Services Router:

```
Router# configure terminal
Router(config)# interface cem 0/0
Router(config-if)# no ip address
Router(config-if)# cem 0
Router(config-if-cem)# dejitter-buffer 10
Router(config-if-cem)# xconnect 10.10.10.10 200 encapsulation mpls
Router(config-if-cem-xconn)# exit
Router(config-if-cem)# exit
Router(config-if)# exit
Router(config)# exit
```

Related Commands

Command	Description
cem	Enters circuit emulation configuration mode.
clear cem	Clears CEM channel statistics.
clear cem	Clears CEM channel statistics.
clear cem	Clears CEM channel statistics.

Command	Description
show cem	Displays CEM channel statistics.

delay-asymmetry

To perform the PTP asymmetry readjustment on a PTP node to compensate for the delay in the network, use the **delay-asymmetry** command in the PTP clock configuration mode. To revert to default setting, use the **no** form of this command.

delay-asymmetry *asymmetry_compensation_offset*
no delay-asymmetry *asymmetry_compensation_offset*

Syntax Description

asymmetry_compensation_offset	Asymetry value of the clock that defines if a one way delay of forward or reverse path occurs.Value ranges from -500000000 to 500000000 nanoseconds.

Command Default

The default asymmetry offset value is zero.

Command Modes

PTP Clock Configuration (for default Telecom profile), Clock-Port Configuration (for G8275.1 Telecom profile)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

The asymmetry compensation offset value can be configured on default, G8275.1 Telecom profile.

The following example demonstrates how to configure the delay asymmetry for ports with default Telecom profile.

```
Router# configure terminal
Router(config)#ptp clock
Router(config-ptp-clk)#clock-port sla slave
Router(config-ptp-port)#clock source 1.1.1.1 delay-asymmetry 300 nanoseconds
```

The following example demonstrates how to configure the delay asymmetry for ports with G8275.1 Telecom profile.

```
Router# configure terminal
Router(config)#ptp clock
Router(config-ptp-clk)#clock-port sla slave
Router(config-ptp-port)#delay-asymmetry 500
```

Related Commands

Command	Description
ptp clock	Creates a Precision Time Protocol clock and specifies the clock mode.
clock-port	Specifies the clocking mode of a Precision Time Protocol clock port.

delay (interface)

To set a delay value for an interface, use the **delay** command in interface configuration mode. To restore the default delay value, use the **no** form of this command.

delay *tens-of-microseconds*
no delay

Syntax Description

tens-of-microseconds	Integer that specifies the delay in tens of microseconds for an interface or network segment. To see the default delay, use the **showinterfaces** command.

Command Default

Default delay values may be displayed with the **showinterfaces**EXEC command.

Command Modes

Interface configuration (config-if) Virtual network interface (config-if-vnet)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Examples

The following example shows how to set a delay of 30,000 microseconds on serial interface 3:

```
Router(config)# interface serial 3
Router(config-if)# delay 3000
```

Related Commands

Command	Description
show interfaces	Displays the statistical information specific to a serial interface.

delay-req interval

To specify a recommended interval for Precision Time Protocol member devices to send delay request messages, use the **delay-reqinterval** command in PTP clock port configuration mode. To remove a delay request interval configuration, use the **no** form of this command.

delay-req interval *interval-value* **unicast**
no delay-req interval *interval-value* **unicast**

Syntax Description

interval-value	Specifies the length of the interval for delay request messages. The intervals are set using log base 2 values, as follows: • 4--1 packet every 16 seconds • 3--1 packet every 8 seconds • 2--1 packet every 4 seconds • 1--1 packet every 2 seconds • 0--1 packet every second • -1--1 packet every 1/2 second, or 2 packets per second • -2--1 packet every 1/4 second, or 4 packets per second • -3--1 packet every 1/8 second, or 8 packets per second • -4--1 packet every 1/16 seconds, or 16 packets per second. • -5--1 packet every 1/32 seconds, or 32 packets per second. • -6--1 packet every 1/64 seconds, or 64 packets per second. The recommended value is -6.
unicast	(Optional) Specifies that the device send PTP delay request messages using unicast mode.

Command Default

The default value is -4 (16 packets per second).

Command Modes

PTP clock-port configuration (config-ptp-port)

Command History

Release	Modification
15.0(1)S	This command was introduced.

Usage Guidelines

This configuration is only required when an interface is in PTP subordinate mode.

Examples

The following example shows how to use the **delay-req** command:

```
Router# configure terminal
Router(config)# ptp clock ordinary domain 0
```

```
Router(config-ptp-clk)# clock-port slaveport slave
Router(config-ptp-port)# delay-req interval 2 unicast
Router(config-ptp-port)# end
```

Related Commands

Command	Description
clock-port	Specifies the mode of a PTP clock port.

description (controller)

To add a description to an E1 or T1 controller or the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers, use the **description**command in controller configuration mode. To remove the description, use the **no**form of this command.

description *string*
no **description**

Syntax Description

string	Comment or description (up to 80 characters) to help you remember what is attached to an interface.

Command Default

No description is added.

Command Modes

Controller configuration

Command History

Release	Modification
10.3	This command was introduced.
11.3	This command was modified to include the CT3IP controller.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **description** command is meant solely as a comment to be put in the configuration to help you remember what certain controllers are used for. The description affects the CT3IP and Multichannel Interface Processor (MIP) interfaces only and appears in the output of the **showcontrollere1**, **showcontrollert1,showcontrollert3**, and**showrunning-config**EXEC commands.

Examples

The following example shows how to add a description for a 3174 controller:

```
Router(config)# controller t1
Router(config-controller)# description 3174 Controller for test lab
```

Related Commands

Command	Description
show controllers e1	Displays information about the E1 links supported by the NPM (Cisco 4000) or MIP (Cisco 7500 series).
show controllers t1	Displays information about the T1 links.
show controllers t3	Displays information about the CT3IP on Cisco 7500 series routers.

description (interface configuration)

To add a description to an interface configuration, use the **description** command in interface configuration mode. To remove the description, use the **no**form of this command.

description *string*
no description

Syntax Description

string	Comment or a description to help you remember what is attached to this interface. This string is limited to 238 characters.

Command Default

No description is added.

Command Modes

Interface configuration

Command History

Release	Modification
9.21	This command was introduced.

Usage Guidelines

The **description** command is meant solely as a comment to be put in the configuration to help you remember what certain interfaces are used for. The description appears in the output of the following EXEC commands:**morenvram:startup-config**, **showinterfaces**, and**moresystem:running-config**

Examples

The following example shows how to add a description for a T1 interface:

```
interface serial 0
 description Fractional T1 line to remote office -- 128 kbps
```

Related Commands

Command	Description
more nvram:startup-config	Displays the startup configuration file contained in NVRAM or specified by the CONFIG_FILE environment variable.
more system:running-config	Displays the running configuration.
show interfaces	Displays statistics for all interfaces configured on the router or access server.

diagnostic level

To turn on power-on diagnostic tests for the network service engines (NSEs) installed in a Cisco 7300 series router, use the **diagnostic level** command in privileged EXEC configuration mode. There is no **no** form of this command.

diagnostic level {**power-on** | **bypass**}

Syntax Description

power-on	Power-on diagnostic tests are performed at system bootup on the NSEs.
bypass	No diagnostic tests are performed. This is the default.

Command Default

No diagnostic tests are performed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EX2	This command was introduced.
12.2(18)S	This command was introduced on Cisco 7304 routers running Cisco IOS Release 12.2 S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to enable power-on diagnostic tests to run on the installed NSEs of a Cisco 7300 series router when the system is booted. It is recommended that you issue this command only if you are experiencing problems with an NSE and are planning on rebooting the router. Issuing this command causes an increase in the boot time.

Examples

The following example shows how to enable diagnostic power-on tests:

```
diagnostic level power-on
```

The following sample output shows the output that is displayed upon system bootup after a power cycle or router crash:

```
.
.
.
System Power On Diagnostics
DRAM Size ....................128 MB
Testing DRAM..................Passed
Level2 Cache .................Present
Testing Level2 Cache (256  KB)Passed
Level3 Cache .................Present
Testing Level3 Cache (1024 KB)Passed
System Power On Diagnostics Complete
```

Note This output is displayed when the system is booting, not when the command is issued.

Related Commands

Command	Description
debug redundancy	Enables NSE redundancy debugging.
show c7300	Displays the types of cards (NSE and line cards) installed in a Cisco 7300 series router.
show redundancy (7300)	Displays redundancy information for the active and standby NSEs.

dial-tdm-clock

To configure the clock source and priority of the clock source used by the time-division multiplexing (TDM) bus on the dial shelf of the Cisco AS5800, use the **dial-tdm-clock** command in global configuration mode. To return the clock source and priority to the default values, use the **no** form of this command.

dial-tdm-clock priority *number* {**external** {**e1** | **t1**} [**120ohm**] | **freerun** | **trunk-slot** *slot* **port** *port*} [**line** {**0** | **1**}]
no dial-tdm-clock priority *number* {**external** {**e1** | **t1**} [**120ohm**] | **freerun** | **trunk-slot** *slot* **port** *port*} [**line** {**0** | **1**}]

Syntax Description

priority *number*	Specifies the priority of the clock source. The range is from 1 to 50. Priority 1 is the highest priority, and 50 is the lowest.
external	Specifies the priority of an external clock source. The external clock source is connected to the front panel of the Dial Shelf Controller (DSC) card.
e1 | **t1**} [**120ohm**]	Specifies priority of the E1 (2.048 MHz) or T1 (1.54 MHz) external clock source. The default value of the external coaxial cable impedance is 75 ohm. Specify the **120ohm**option if a 120 ohm coaxial cable is connected.
freerun	Specifies the priority of the local oscillator clock source.
trunk-slot *slot*	Specifies the priority of the trunk card to provide the clock source. The slot number is from 0 to 5 (these are the only slots capable of providing clock sources).
port *port*	Specifies the controller number on the trunk used to provide the clock source. The port number is from 0 to 28. The T1 and E1 trunk cards each have 12 ports. The T3 trunk card has 28 ports.
line {**0** | **1**	(Optional) Specifies the optical port. If the physical optical port is 0, the**line** value is also 0.

Command Default

If no clock sources are specified, the software selects the first available good clock source on a trunk port.

Command Modes

Global configuration

Command History

Release	Modification
11.3(2)AA	This command was introduced.
12.2(15)T	The **line** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The TDM bus in the backplane on the dial shelf must be synchronized to the T1/E1 clocks on the trunk cards. The DSC card on the dial shelf provides hardware logic to accept multiple clock sources as input and use one of them as the primary source to generate a stable, PPL synchronized output clock. The input clock can be any of the following sources:

- Trunk port in slots 0 through 5 (up to 12 can be selected (two per slot)
- An external T1 or E1 clock source fed directly through a connector on the DSC card
- A free running clock from an oscillator in the clocking hardware on the DSC card

The clock commands are listed in the configuration file with the highest priority listed first.

If the current primary clock source is good, specifying another clock source of higher priority does not cause the clock source to switch to the higher priority clock source. The new higher priority clock source is used as a backup clock source. This prevents switching of the clock source as you enter multiple dial-tdm-clock priority configuration commands in random order. Also, it is important not to disturb the existing clock source as long as it is good. To force the new higher priority clock source to take over from a currently good primary clock source, configure the new clock source and use the **no** dial-tdm-clock priority command to remove the current primary clock source.

To display the current primary and backup clocks along with their priorities, use the **showdial-shelfclocks**EXECcommand.

Examples

In the following example, an external clock source is set at priority 1 and the trunk card in slot 4, port 1 is set at priority 5:

```
Router(config)# dial-tdm-clock priority 1 external t1
Router(config)# dial-tdm-clock priority 5 trunk-slot 4 port 1
Router(config)# exit
```

Related Commands

Command	Description
show dial-shelf	Displays information about the dial shelf, including clocking information.

dot1q tunneling ethertype

To define the Ethertype field type used by peer devices when implementing Q-in-Q VLAN tagging, use the **dot1qtunnelingethertype**command in interface configuration mode. To remove the VLAN tag Ethertype, use the **no** form of this command.

no dot1q tunneling ethertype{*0x88A8 0x9100 0x9200*}
no dot1q tunneling ethertype

Syntax Description

0x88A8 |0x9100|0x9200	Type of Ethertype field.

Command Default

The Ethertype field used by peer devices when implementing Q-in-Q VLAN tagging is 0x8100.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.3(7)XI1	This command was implemented on the Cisco 10000 series routers.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2.

Usage Guidelines

Use the **dot1qtunnelingethertype** command if the peer switching devices are using an Ethertype field value of 0x9100 or 0x9200. All Cisco switching devices use the default Ethertype field value of 0x88A8. The Cisco 10000 series router also supports the 0x9200 Ethertype field value.

Note On the Cisco 10000 series router, the Ethertype field for the outer VLAN ID can be changed, but the Ethertype field for the inner VLAN ID cannot be changed.

This command is used with the IEEE 802.1Q-in-Q VLAN Tag Termination feature in which double VLAN tagging is configured using the **encapsulationdot1q** command. 802.1Q double tagging allows a service provider to use a single VLAN to support customers who have multiple VLANs.

Examples

The following example shows how to configure an Ethertype field as 0x9100:

```
Router(config
)
# interface gigabitethernet 1/0/0
Router(config
-if)#
 dot1q tunneling ethertype 0x9100
```

The following example shows how to configure an Ethertype field as 0x9200 on a Cisco 10000 series router:

```
Router(config)# interface gigabitethernet 1/0/0
Router(config-if)# dot1q tunneling ethertype 0x9200
```

Related Commands

Command	Description
encapsulation dot1q	Enables 802.1Q encapsulation of traffic on a specified subinterface or range of subinterfaces.
interface	Configures an interface and enters interface configuration mode.

down-when-looped

To configure an interface to inform the system that it is down when loopback is detected, use the **down-when-looped**command in interface configuration mode.

down-when-looped

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is valid for High-Level Data Link Control (HDLC) or PPP encapsulation on serial and High-Speed Serial Interface (HSSI) interfaces.

This command does not have a **no** form.

Note

- This command cannot be enabled when default speed or 1000BaseT advertisement is enabled on the GMII interface.
- 1000BaseT advertisement cannot be configured when down-when-looped is enabled.

Backup Interfaces

When an interface has a backup interface configured, it is often desirable that the backup interface be enabled when the primary interface is either down or in loopback. By default, the backup is enabled only if the primary interface is down. By using the **down-when-looped** command, the backup interface will also be enabled if the primary interface is in loopback.

Testing an Interface with the Loopback Command

If testing an interface with the loopback command, or by placing the DCE into loopback, the **down-when-looped** command should not be configured; otherwise, packets will not be transmitted out the interface that is being tested.

Examples

The following example shows how to configure interface serial 0 for HDLC encapsulation. The interface is then configured to let the system know that it is down when in loopback mode.

```
Router(config)# interface serial0
```

```
Router(config-if)# encapsulation hdlc
Router(config-if)# down-when-looped
```

Related Commands

Command	Description
backup interface	Configures an interface as a secondary or dial backup interface.
loopback (E3 controller)	Diagnoses equipment malfunctions between an interface and a device.

ds0-group (J1 controller)

To configure channelized J1 time slots, use the**ds0-group**commandincontroller configuration mode. To remove the DS0 group, use the**no** form of this command.

ds0-group *ds0-group-no* **timeslots** *timeslot-list* **type** *external-signaling*
no ds0-group *ds0-group-no* **timeslots** *timeslot-list* **type** *external-signaling*

Syntax Description

ds0-group-no	Specifies the DS0 group number.
timeslots *timeslot-list*	Specifies the DS0 time slot range of values from 1 to 31 for J1 interfaces. Time slot 16 is reserved for signaling.
type *external-signaling*	Specifies that the signaling traffic comes from an outside source. The signaling method selection for type depends on the connection that you are making.

Command Default

No DS0 group is defined.

Command Modes

Controller configuration

Command History

Release	Modification
11.2	This command was originally the **cas-group** command.
12.0(1)T	The **cas-group** command was introduced for the Cisco 3600 series.
12.0(5)XE	The command was renamed**ds0-group** on the Cisco AS5300 and on the Cisco 2600 and Cisco 3600 series.
12.0(7)T	The command was integrated into the Cisco IOS Release 12.0(7)T.
12.2(8)T	The command was introduced as a J1 configuration command for the Cisco 2600 and Cisco 3600 series.

Usage Guidelines

The ds0-group command replaces the existing cas-group command. Making the command generic allows flexibility and scalability. It is not restricted to channel associated signaling (CAS) or channel bundling.

The **ds0-group** command automatically creates a logical voice port that is numbered as follows on Cisco 2600 and Cisco 3600 series routers: *slot*/*port***:***ds0-group-no*. Although only one voice port is created for each group, applicable calls are routed to any channel in the group.

Examples

The following example is sample output from the **showcontrollersj1**command on the Cisco 3660 series after channelized J1 time slots have been configured:

```
Router(config-controller)# ds0-group 1 timeslots 1-15,17-31 type e&m-wink-start

Router(config-controller)# end
Router# show controllers j1
*Mar  1 03:12:26.259: %LINK-3-UPDOWN: Interface recEive and transMit3/0:0(1), cp
*Mar  1 03:12:26.259: %LINK-3-UPDOWN: Interface recEive and transMit3/0:0(2), cp
```

```
*Mar  1 03:12:26.259: %LINK-3-UPDOWN: Interface recEive and transMit3/0:0(3), cp
*Mar  1 03:12:26.259: %LINK-3-UPDOWN: Interface recEive and transMit3/0:0(4), cp
*Mar  1 03:12:26.259: %LINK-3-UPDOWN: Interface recEive and transMit3/0:0(5), cp
*Mar  1 03:12:26.259: %LINK-3-UPDOWN: Interface recEive and transMit3/0:0(6), cp
*Mar  1 03:12:26.259: %LINK-3-UPDOWN: Interface recEive and transMit3/0:0(7), cp
*Mar  1 03:12:26.259: %LINK-3-UPDOWN: Interface recEive and transMit3/0:0(8), cp
*Mar  1 03:12:26.259: %LINK-3-UPDOWN: Interface recEive and transMit3/0:0(9), cp
*Mar  1 03:12:26.259: %LINK-3-UPDOWN: Interface recEive and transMit3/0:0(10), p
*Mar  1 03:12:26.259: %LINK-3-UPDOWN: Interface recEive and transMit3/0:0(11), p
*Mar  1 03:12:26.259: %LINK-3-UPDOWN: Interface recEive and transMit3/0:0(12), p
*Mar  1 03:12:26.259: %LINK-3-UPDOWN: Interface recEive and transMit3/0:0(13), p
*Mar  1 03:12:26.259: %LINK-3-UPDOWN: Interface recEive and transMit3/0:0(14), p
*Mar  1 03:12:26.259: %LINK-3-UPDOWN: Interface recEive and transMit3/0:0(15), p
*Mar  1 03:12:26.259: %LINK-3-UPDOWN: Interface recEive and transMit3/0:0(17), p
*Mar  1 03:12:26.259: %LINK-3-UPDOWN: Interface recEive and transMit3/0:0(18), p
*Mar  1 03:12:26.259: %LINK-3-UPDOWN: Interface recEive and transMit3/0:0(19), p
*Mar  1 03:12:26.259: %LINK-3-UPDOWN: Interface recEive and transMit3/0:0(20), p
*Mar  1 03:12:26.259: %LINK-3-UPDOWN: Interface recEive and transMit3/0:0(21), p
*Mar  1 03:12:26.259: %LINK-3-UPDOWN: Interface recEive and transMit3/0:0(22), p
*Mar  1 03:12:26.259: %LINK-3-UPDOWN: Interface recEive and transMit3/0:0(23), p
*Mar  1 03:12:26.259: %LINK-3-UPDOWN: Interface recEive and transMit3/0:0(24), p
*Mar  1 03:12:26.263: %LINK-3-UPDOWN: Interface recEive and transMit3/0:0(25), p
*Mar  1 03:12:26.263: %LINK-3-UPDOWN: Interface recEive and transMit3/0:0(26), p
*Mar  1 03:12:26.263: %LINK-3-UPDOWN: Interface recEive and transMit3/0:0(27), p
*Mar  1 03:12:26.263: %LINK-3-UPDOWN: Interface recEive and transMit3/0:0(28), p
*Mar  1 03:12:26.263: %LINK-3-UPDOWN: Interface recEive and transMit3/0:0(29), p
*Mar  1 03:12:26.263: %LINK-3-UPDOWN: Interface recEive and transMit3/0:0(30), p
*Mar  1 03:12:26.263: %LINK-3-UPDOWN: Interface recEive and transMit3/0:0(31), p
```

Related Commands

Command	Description
ds0 busyout	Busyouts one or more signal level 0s (DS0s).

dsl-group

To create and configure a digital subscriber line (DSL) group, and enter config-controller-dsl-group mode, or to automatically configure an ATM group, use the **dsl-group**command in configuration controller mode. To disable the DSL group, use the **no** form of this command.

dsl-group [**pairs**] [{[*number*] **pairs** *link-number* | **auto** [{**default** | **exit** | **no** | **shdsl** {**4-wire** | **annex**}}]}] [**efm-bond**]
no dsl-group [**pairs**] [{[*number*] **pairs** *link-number* | **auto** [{**default** | **exit** | **no** | **shdsl** {**4-wire** | **annex**}}]}] [**efm-bond**]

Syntax Description

pairs	(Optional) Defines the DSL wire pairs.
number	(Optional) DSL group number. The DSL group number can be one of the following numbers: • 0 • 1
efm-bond	(Optional) Defines the DSL group as Ethernet First Mile (EFM) group bonding group.

link-number	(Optional) Link number of the pair. Link number options are limited to one of the following choices, based on the hardware interface and the desired DSL group: **HWIC-4SHDSL-E** EFM-bond DSL Group • 0 • 1 • 2 • 3 • Any combination of the numbers 0, 1, 2, and 3 1-Pair DSL Group • 0 • 1 • 2 • 3 In the case of 1-pair DSL group (2-wire), only one pair needs to be configured. **HWIC-4SHDSL** IMA DSL Group • 0 • 1 • 2 • 3 • Any combination of the numbers 0, 1, 2, and 3

	M-Pair DSL Group • 0-1 • 0-2 • 0-3 2-Pair DSL Group • 0-1 • 2-3 1-Pair DSL Group • 0 • 1 • 2 **HWIC-2SHDSL** DSL Group 0 • 0 • 0-1 DSL Group 1 • 1
auto	(Optional) Automatically assigns the Central Office's (CO) wire configuration to an ATM DSL group on the Customer Premise Equipment (CPE).
default	(Optional) Sets a command to the default values.
exit	(Optional) Exits DSL group command mode.
no	(Optional) Negates a command or set its defaults.
shdsl	(Optional) Configures the symmetric g.shdsl.
4-wire	(Optional) Configures the 4-wire symmetric g.shdsl.
annex	(Optional) Configures the annex symmetric g.shdsl.

Command Default

No DSL group is defined or automatically configured.

Command Modes

Configuration controller (config-controller)

Configuration controller DSL group (config-controller-dsl-group)

Command History

Release	Modification
12.4(15)T	This command was introduced for the Cisco HWIC-4SHDSL and HWIC-2SHDSL running on the Cisco 1841 router and the Cisco 2800 and 3800 series access routers.
15.1(1)T	This command was modified to support automatic configuration of Cisco HWIC-4SHDSL and HWIC-2SHDSL running on the Cisco 1841 router and the Cisco 2800 and 3800 series access routers. Added **dsl-grouppairs***link-number* [**efm-bond**] for the Cisco HWIC-4SHDSL-E.
15.1(1)T1	This command was modified. The auto configuration options **default**,**exit**,**no**, and **shdsl**were added to the dsl-group.

Usage Guidelines

Use the **dsl-group** command in configuration controller mode to define the DSL group, and manually configure the DSL group from configuration controller DSL group mode. Use the **dsl-groupauto** command to automatically adopt the Central Office (CO) wire configuration on an ATM DSL group. Use the **dsl-grouppairs** to define the DSL group as Ethernet First Mile (EFM) group bonding group.

Note Automatic configuration is not supported on IMA groups.

Automatic configuration is limited to only one DSL group and ATM interface. After a group is automatically configured, no other group can be created. All manually created groups must be deleted before creating an automatic configuration group.

Examples

The following example shows how to use the dsl-group command to create an IMA-DSL group and enter configuration controller DSL group mode:

```
Router(config-controller)# dsl-group 1 pairs 0-1 ima
Router(config-controller-dsl-group)#
Sep 14 13:15:40.285:%HWIC_SHDSL-5-DSLGROUP_UPDOWN: SHDSL 0/2/0 dsl-group(1) state changed
to down.
Sep 14 13:15:42.285:%LINK-3-UPDOWN: Interface ATM0/2/IMA1, changed state to down
Sep 14 13:15:43.285:%LINEPROTO-5-UPDOWN: Line protocol on Interface ATM0/2/IMA1, changed
state to down
```

The following example shows how to use the dsl-group auto command to automatically adopt the Central Office (CO) configuration on an ATM group:

```
Router(config-controller)# dsl-group auto
Router(config-controller-dsl-group-auto)#
*May 14 18:56:33.136: %HWIC_SHDSL-5-DSLGROUP_UPDOWN: SHDSL 0/0/0 dsl-group(0) state changed
 to down.
*May 14 18:56:35.136: %LINK-3-UPDOWN: Interface ATM0/0/0, changed state to down
*May 14 18:56:36.136: %LINEPROTO-5-UPDOWN: Line protocol on Interface ATM0/0/0,
changed state to down
```

The following example shows how to configure a single-pair DSL group and enters the configuration controller DSL group mode:

```
Router(config-controller)# dsl-group pairs 0
Router(config-controller-dsl-group)#
```

The following example shows how to create a 4-pair EFM bonding group:

```
Router(config-controller)# dsl-group pairs 0-3 efm-bond
Router(config-controller-dsl-group)#
```

Related Commands

Command	Description
controller shdsl	Configures a controller for SHDSL mode and enters configuration controller mode.
ima group	Defines physical links as IMA group members.
ima group clock-mode	Sets the clock mode for an IMA group.
ima link	Defines physical links in an IMA group.
shdsl 4-wire mode enhanced	Defines the SHDSL to use enhanced mode in a 2-pair DSL group.
shdsl annex	Defines the SHDSL G.991.2 standard.
shdsl rate	Defines the SHDSL rate.
show controller shdsl	Displays the status of the controller that is configured for SHDSL mode.

dsl-mode shdsl symmetric annex

To specify the operating mode of the digital subscriber line (DSL) controller, use the **dsl-mode shdsl symmetric annex**command in controller configuration mode.

To specify the line coding type of the DSL controller, use the **dsl-mode shdsl symmetric annex coding**command in controller configuration mode. To return the DSL to the default Annex A, use the **no** form of the command.

dsl-mode shdsl symmetric annex mode [**coding type**]
no dsl-mode shdsl symmetric annex mode [**coding type**]

Syntax Description

mode	Sets the DSL operating mode. The valid values are: • **a** : Supports Annex A of the G.991.2 standard for North America. This is the default. • **b** : Supports Annex B of the G.991.2 standard for Europe. • **a-b** : Supports Annex A or B. For CPE mode only. Not supported in CO mode. Selected when the line trains. • **a-b-anfp** : Supports Annex A or B-ANFP. For CPE mode only. Not supported in CO mode. Selected when the line trains. • **b-anfp** : Supports Annex B-ANFP. • f: Supports Annex F, 2-wire mode, line 0 only. • f-g: Supports Annex F-G, 2-wire mode, line 0 only. • g: Supports Annex G, 2-wire mode, line 0 only.
coding	TCPAM line coding.
Type	The valid values are: • 16bit-TCPAM: Sets the line coding to16 bit-TCPAM. • 32bit-TCPAM: Sets the line coding to 32 bit-TCPAM. • AUTO-TCPAM: Detects the central office coding type.

The annex defaults to A for North America.

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
12.3(4)XD	This command was introduced on Cisco 2600 series and Cisco 3700 series routers.
12.3(4)XG	This command was integrated into the Cisco IOS Release 12.3(4)XG on the Cisco 1700 series routers.

Release	Modification
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T on Cisco 2600 series, Cisco 3631, and Cisco 3700 series routers.
12.3(11)T	Support for the following additional annex parameters was integrated into Cisco IOS Release 12.3(11)T to support Cisco 1700, Cisco 2600, Cisco 2800, Cisco 3700, and Cisco 3800 series routers: • **b** • **a-b** • **a-b-anfp** • **b-anfp**
12.3(14)T	This command was implemented on Cisco 1800 series routers.
12.4(15)T	Support for the following additional annex parameters was integrated into Cisco IOS Release 12.X(X)T to support Cisco to support Cisco 1700, Cisco 2600, Cisco 2800, Cisco 3700, and Cisco 3800 series routers: • f • f-g • g
12.4(20)T	Support for **coding** *type* parameters was added.

Usage Guidelines

This command is used to configure the DSL controller interface to operate in a specified DSL mode and to set regional operating parameters. The **shdsl** keyword is used to set the mode to SHDSL and configures multirate, high-speed DSL per ITU G.991.2. The **symmetric** keyword configures the controller to symmetric mode. The **annex** keyword configures the controller to use regional operating parameters. The regional operating parameters default to North America. The coding keyword configures the controller Trellis Encoded Pulse Amplitude Modulation (TCPAM) line coding type.

Examples

The following example displays the use of the **controller dsl 0/0**commandto configure the controller in the router configured on the central office (CO) side. Use the **dsl-mode shdsl symmetric annex b**command to configure the controller for multirate, high-speed DSL with symmetric mode for European operating parameters.

```
Router# configure terminal

Router(config)# controller dsl 0/0
Router(config-controller)# line-term co
Router(config-controller)# dsl-mode shdsl symmetric annex b
Router(config-controller)# mode atm
Router(config-controller)#
00:22:07: %CONTROLLER-5-UPDOWN: Controller DSL 0/0, changed state to down
Router(config-controller)# line-mode 4-wire
00:23:25: %CONTROLLER-5-UPDOWN: Controller DSL 0/0, changed state to up
00:23:31: %LINK-3-UPDOWN: Interface ATM0/0, changed state to up
00:23:32: %LINEPROTO-5-UPDOWN: Line protocol on Interface ATM0/0, changed state to up
```

The following example uses the **dsl-mode shdsl symmetric annex command to configure the controller for 2-wire line 0, annex F, AUTO-TCPAM line coding.**

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# controller dsl 0
Router(config-controller)# line-mode 2-wire line-zero
Router(config-controller)# dsl-mode shdsl symmetric annex f coding ?
 16bit-TCPAM  16bit-TCPAM line coding
 32bit-TCPAM  32bit-TCPAM line coding
 AUTO-TCPAM   AUTO-TCPAM line coding
Router(config-controller)# dsl-mode shdsl symmetric annex f coding auto-tcpam
Router(config-controller)#
Router#
```

Related Commands

Command	Description
controller dsl	Configures the DSL controller.

dsu bandwidth

To specify the maximum allowable bandwidth used by a T3 or E3 controller or the PA-T3 and PA-E3 port adapters, use the **dsubandwidth**command in interface configuration mode. To return to the default bandwidth, use the **no** form of this command.

dsu bandwidth *kbps*
no dsu bandwidth

Syntax Description

kbps	Maximum bandwidth, in kbps. Range is from 22 to 44736. Default values are as follows: • 34,010 for E3 or PA-E3 • 44,210 for T3 • 44,736 for PA-T3 • 34,368 kbps for E3 on a Cisco_10000 Series Router • 44,210 kbps for T3 on a Cisco_10000 Series Router

Command Default

34,010 kbps

44,210 kbps

44,736 kbps

34,368 kbps for E3

44,210 kbps for T3

Command Modes

Interface configuration

Command History

Release	Modification
11.1CA	This command was introduced.
12.2(11)YT	This command was integrated into Cisco IOS Release 12.2(11)YT and implemented on the following platforms: Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3660 series, Cisco 3725, and Cisco 3745 routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Local and Remote Bandwidths

The local interface configuration must match the remote interface configuration. For example, if you reduce the maximum bandwidth to 16,000 on the local port, you must also do the same on the remote port.

The **dsubandwidth**command reduces the bandwidth by padding the E3 and T3 frame.

Verifying DSU Bandwidth

To verify the data service unit (DSU) bandwidth configured on the interface, use the show interfaces serial user EXEC command.

G.751 Framing

When G.751 framing is used, DSU bandwidth can be used to select a payload subrate from 34,010 kbps down to 22 kbps. Before framing bypass can be used, a DSU bandwidth of 34,010 kbps must be configured.

Continuous Range of Bandwidth

Even though Cisco_IOS software allows you to configure a continuous range of bandwidths in subrate modes, vendors support bandwidths only in quantums (for example, in an E3 digital link, bandwidth must be in multiples of 358 kbps). Therefore, the software sets the user-configured bandwidth to the closest vendor-supported bandwidth. Use the show interfaces serial slot/port command to display the actual bandwidth that is configured.

Subrates

The user-configured subrate mode, subrate bandwidth, actual subrate bandwidth configured, and scramble configuration are displayed near the end of the show interfaces serial command output.

DSU Modes and Vendor-Supported Bandwidths

The following table shows DSU modes and vendor-supported bandwidths.

Mode	DSU	Bandwidth Range	Bandwidth Multiples
0	Digital Link or Cisco	358-34,010 kbps for E3 300-44,210 kbps for T3	358 kbps 300.746 kbps
1	ADC Kentrox T3/E3 IDSU	1000-34,010 kbps for E3 1500-44,210 kbps for T3	500 kbps 500 kbps
2	Larscom Access T45	3100-44,210 kbps	3158 kbps
3	Adtran T3SU 300	75-44,210 kbps	75.186 kbps
4	Verilink HDM 2182	1500-44,210 kbps	1579 kbps

Examples

The following example sets the maximum allowable DSU bandwidth to 16,000 kbps on interface 1/0/0:

```
Router(config)# interface serial 1/0/0
Router(config-if)# dsu bandwidth 16000
```

The following example shows the user-configured subrate bandwidth and the actual configured subrate bandwidth as displayed in the output of the show interfaces serial command:

```
Router# show interfaces serial
Serial1/0 is up, line protocol is up
```

```
  Hardware is DSXPNM Serial
  MTU 1500 bytes, BW 44210 Kbit, DLY 20000 usec,
     reliability 253/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, crc 16, loopback not set
  Keepalive not set
  DTR is pulsed for 0 seconds on reset, Restart-Delay is 1637167 secs
  Last input 04:59:04, output 04:59:04, output hang never
  Last clearing of "show interface" counters 00:00:02
  Input queue:0/75/0/0 (size/max/drops/flushes); Total output drops:0
  Queueing strategy:fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
 DSU mode 0, bandwidth 34010, real bandwidth 34010, scramble 0
```

Related Commands

Command	Description
show interfaces serial	Displays information that is specific to the interface hardware.

dsu mode

To specify the interoperability mode used by a T3 or E3 controller or the PA-T3 and PA-E3 port adapters, use the **dsumode**command in interface configuration mode. To return to the default mode, use the **no** form of this command.

dsu mode {**0** | **1** | **2** | **3** | **4**}
no dsu mode

Cisco 10000 Series Router
dsu mode {**adtran** | **cisco** | **digital-link** | **kentrox** | **larscom** | **verilink-highbit** | **verilink-lowbit**}
no dsu mode

Syntax Description

0	Sets the interoperability mode to 0. This is the default. • Specify mode 0 to connect an E3 controller to another E3 controller or to a Digital Link data service unit (DSU) DL3100. • Specify mode 0 to connect a PA-E3 port adapter to another PA-E3 port adapter or to a DL3100. • Specify mode 0 to connect a PA-T3 port adapter to another PA-T3 port adapter or to a DL3100.
1	Sets the interoperability mode to 1. Specify mode 1 to connect an E3 or T3 controller or a PA-E3 or PA-T3 port adapter to a Kentrox DSU.
2	Sets the interoperability mode to 2. Specify mode 2 to connect a T3 controller or a PA-T3 port adapter to a Larscom DSU.
3	Sets the interoperability mode to 3. Specify mode 3 to connect a T3 controller to an Adtran T3SU 300.
4	Sets the interoperability mode to 4. Specify mode 4 to connect a T3 controller to a Verilink HDM 2182.
adtran	Connects a T3 interface to an Adtran DSU.
cisco	Connects an E3 or T3 interface to a Cisco DSU.
digital-link	Connects an E3 or T3 interface to a Digital Link DSU.
kentrox	Connects an E3 or T3 interface to a Kentrox DSU.
larscom	Connects a T3 interface to a Larscom DSU.
verilink-highbit	Connects a T3 interface to a Verilink High Bit DSU.
verilink-lowbit	Connects a T3 interface to a Verilink Low Bit DSU.

Command Default

0

cisco

Command Modes

Interface configuration

Command History

Release	Modification
11.1CA	This command was introduced.
12.2(11)YT	This command was integrated into Cisco IOS Release 12.2(11)YT and implemented on the following platforms for E3 and T3 controllers: Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3660 series, Cisco 3725, and Cisco 3745 routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Scrambling Support in DSU Mode 1

DSU mode 1 refers to Kentrox mode. If DSU mode is used on a T3 serial interface and the bandwidth is greater than or equal to 35,000 bits per second (bps), the scrambling option is not supported. Likewise, if DSU mode 1 is used for an E3 serial interface and the bandwidth is greater than or equal to 24,510 bps, scrambling is not supported.

Match Local and Remote DSU Configurations

The local interface configuration must match the remote interface configuration. For example, if you define the DSU interoperability mode as 1 on the local port, you must also do the same on the remote port.

Know the DSU Type

You must know what type of DSU is connected to the remote port to determine if it interoperates with an E3 or T3 controller or a PA-E3 or PA-T3 port adapter. The **dsumode** command enables and improves interoperability with other DSUs.

Verify DSU Mode

To verify the DSU mode configured on the interface, use the **showcontrollersserial** or **showinterfacesserial** user EXEC commands.

Cisco 10000 Series Router

Only Cisco, Digital Link, and Kentrox DSUs are supported on E3 interfaces.

Examples

Setting DSU Mode

The following example sets the DSU mode to 1 on interface 1/0/0:

```
Router(config)# interface serial 1/0/0
Router(config-if)# dsu mode 1
```

Serial Interface in DSI Mode 1

The following example shows the configuration for a serial interface configured in DSU mode 1. The bandwidth is set higher than that supported by the Kentrox firmware allows for scrambling. therefore, the scrambling option is not supported in this configuration.

```
Router(config
)#
 interface serial 1/0/0
Router(config-if)# mtu 4474
Router(config-if)# ip address 192.168.93.114 255.255.255.252
Router(config-if)# ip mtu 4470
Router(config-if)# dsu mode 1
Router(config-if)# dsu bandwidth 44210
```

Cisco 10000 Series Router

The following example sets the DSU mode to cisco:

```
Router(config)# interface serial 1/0/0
Router(config-if)# dsu mode cisco
```

Related Commands

Command	Description
show controllers	Displays information about the controllers.
show interfaces	Displays statistics for all interfaces configured on the router.

dte-invert-txc

To invert the transmit external clock (TXC) signal received from the DCE when the device is operating as a DTE, use the **dte-invert-txc** command in interface configuration mode. If the DCE accepts serial clock transmit external (SCTE) signal when the device is operating as a DTE, use the **no** form of this command.

dte-invert-txc
no dte-invert-txc

Syntax Description

This command has no arguments or keywords.

Command Default

The TXC signal is not inverted.

Command Modes

Interface configuration

Command History

Release	Modification
9.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command if the DCE cannot receive SCTE from the DTE, the data is running at high speeds, and the transmission line is long. The **dte-invert-txc** command prevents phase shifting of the data with respect to the clock.

On the Cisco 4000 series, you can specify the serial Network Processor Module timing signal configuration. When the board is operating as a DTE, the **dte-invert-txc** command inverts the TXC clock signal it gets from the DCE that the DTE uses to transmit data.

If the DCE accepts SCTE from the DTE, use **nodte-invert-txc**.

Examples

The following example inverts the TXC on serial interface 0:

```
Router(config)# interface serial 0
Router(config-if)# dte-invert-txc
```

duplex

To configure the duplex operation on an interface, use the **duplex** command in interface configuration mode. To return to the default configuration, use the **no** form of this command.

duplex {**full** | **half** | **auto**}
no duplex

Syntax Description

full	Specifies full-duplex operation.
half	Specifies half-duplex operation.
auto	Enables autonegotiation. The interface automatically operates at half-duplex or full-duplex mode depending on environmental factors, such as the type of media and the transmission speeds for the peer routers, hubs, and switches used in the network configuration.

Command Default

Half-duplex mode is enabled.

For the 4-port 10/100 Fast Ethernet Shared Port Adapter (SPA) and the 2-port 10/100/1000 Gigabit Ethernet SPA on the Cisco 7304 router, autonegotiation is enabled. The command is set to **auto**.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.2(10)P	This command was introduced.
12.2S	This command was integrated into Cisco IOS Release 12.2S.
12.2(14)SX	This command was implemented on the Supervisor Engine 720.
12.2(17d)SXB	This command was integrated into Cisco IOS Release 12.2 SXB.
12.2(20)S2	This command was implemented on the 4-port 10/100 Fast Ethernet SPA and the 2-port 10/100/1000 Gigabit Ethernet SPA on the Cisco 7304 router.
Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S.
15.2(02)SA	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

To use the autonegotiation capability (that is, to automatically detect speed and duplex modes), you must set both the **speed** command and the **duplex** command to **auto**.

Cisco Cloud Services Router 1000V Series

Cisco Cloud Services Router 1000V Series does not support the **duplex** command.

Duplex Options and Interfaces

The table below lists the supported command options by interface type.

Table 12: Supported Duplex Command Options

Interface Type	Supported Syntax	Default Setting	Usage Guidelines
10/100-Mbps module	**duplex** [**half** | **full**]	See the "Usage Guidelines" column.	Run the **no duplex auto** command to set the speed to **auto**. If the speed is set to **10** or **100**, without configuring the duplex setting, the duplex is set to **half**.
100-Mbps fiber modules	**duplex** [**half** | **full**]	**half**	
Gigabit Ethernet interfaces	**duplex full**	**full**	
10-Mbps ports	**duplex** [**half** | **full**]	**half**	

If the transmission speed on a 16-port RJ-45 Gigabit Ethernet port is set to 1000, the duplex mode is set to full. If the transmission speed is changed to 10 or 100, the duplex mode stays at half duplex. You must configure the correct duplex mode when the transmission speed is changed to 10 or 100 from 1000.

Gigabit Ethernet is full duplex only. You cannot change the mode on Gigabit Ethernet ports.

When manually configuring the interface speed to either 10 or 100-Mbps, you should also configure the duplex mode on the interface.

Caution Changing the interface speed and duplex mode configuration might shut down and reenable the interface during reconfiguration.

4-Port 10/100 Fast Ethernet SPA and 2-Port 10/100/1000 Gigabit Ethernet SPA on the Cisco 7304 Router

The **duplex** command is applied to the SPA interfaces that use the RJ-45 media. Gigabit Ethernet interfaces using fiber media support full-duplex mode only and use the **negotiation** command to enable and disable autonegotiation.

To enable the autonegotiation capability on an RJ-45 interface, you must set either the **speed** command or the **duplex** command to **auto**. The default configuration is that both commands are set to **auto**.

Note For the Cisco AS5300, the **duplex** {**full** | **half** | **auto**} command syntax replaces the **duplex** commands—**half-duplex** and **full-duplex**. Cisco 7600 series routers can automatically negotiate the interface speed and the duplex mode only if one of the connected interfaces are configured to **auto**.

The table below describes the interface behavior for different combinations of the **duplex** and **speed** command settings. The specified **duplex** command configured with the specified **speed** command produces the resulting system action.

If you specify both **duplex** and **speed** settings other than **auto** on an RJ-45 interface, autonegotiation is disabled for the interface.

Note If you need to force an interface port to operate with certain settings and, therefore, need to disable autonegotiation, you must be sure that the remote link is configured with compatible link settings for proper transmission including the support of flow control on the link.

Note Every interface on a 4-port 10/100 Fast Ethernet SPA supports transmission of pause frames to stop packet flow when the Modular Services Card (MSC) is full. You cannot disable flow control for an interface on the 4-port 10/100 Fast Ethernet SPA. Hence, the flow control support is not configurable, but it is advertised during autonegotiation. If you disable autonegotiation, you must be sure that the remote device is configured to support flow control because flow control is automatically enabled for all interfaces on the 4-port 10/100 Fast Ethernet SPA.

Table 13: Relationship Between duplex and speed Commands

duplex Command	speed Command	Resulting System Action
duplex auto	**speed auto**	Autonegotiates both speed and duplex modes. The interface advertises the capability for the following link settings: • 10 Mbps and half duplex • 10 Mbps and full duplex • 100 Mbps and half duplex • 100 Mbps and full duplex • 1000 Mbps and half duplex • 1000 Mbps and full duplex
duplex auto	**speed 10** or **speed 100** or **speed 1000**	Autonegotiates the duplex mode. The interface advertises the capability for the configured speed with the capability for both half-duplex or full-duplex mode. For example, if the **speed 100** command is configured with **duplex auto**, then the interface advertises the following capability: • 100 Mbps and half duplex • 100 Mbps and full duplex

duplex Command	speed Command	Resulting System Action
duplex half or **duplex full**	**speed auto**	Autonegotiates the speed. The interface advertises the capability for duplex mode for Fast Ethernet interfaces at a speed of 10-Mbps and 100-Mbps, and Gigabit interfaces at 10-Mbps, 100-Mbps, and 1000-Mbps. For example, if the **duplex full** command is configured with the **speed auto** command, then the interface advertises the following capability: • 10 Mbps and full duplex • 100 Mbps and full duplex • 1000 Mbps and full duplex (Gigabit Ethernet interfaces only)
duplex half	**speed 10**	Forces 10-Mbps speed and the half-duplex operation, and disables autonegotiation on the interface.
duplex full	**speed 10**	Forces a speed of 10-Mbps and the full-duplex operation, and disables autonegotiation on the interface.
duplex half	**speed 100**	Forces a speed of 100-Mbps and the half-duplex operation, and disables autonegotiation on the interface.
duplex full	**speed 100**	Forces a speed of 100-Mbps and the full-duplex operation, and disables autonegotiation on the interface.
duplex half	**speed 1000**	Forces a speed of 1000-Mbps and the half-duplex operation, and disables autonegotiation on the interface (Gigabit Ethernet only).
duplex full	**speed 1000**	Forces a speed of 1000-Mbps and the full-duplex operation, and disables autonegotiation on the interface (Gigabit Ethernet only).

Examples

The following example shows how to configure a full-duplex operation on a Cisco AS5300 router:

```
Device(config)# interface fastethernet 0
Device(config-if)# duplex full
```

The following example shows how to specify the advertisement of only half-duplex support and either 10-Mbps or 100-Mbps capability during autonegotiation for the second interface (port 1) on the SPA located in the bottom subslot (1) of the MSC that is installed in slot 2 of the Cisco 7304 router:

```
Device# configure terminal
Device(config)# interface fastethernet 2/1/1
Device(config-if)# duplex half
Device(config-if)# speed auto
```

With this configuration, the interface advertises the following capabilities during autonegotiation:

- 10 Mbps and half duplex
- 100 Mbps and half duplex

Note Flow control support is always advertised when autonegotiation is enabled.

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
interface fastethernet	Selects a particular Fast Ethernet interface for configuration.
interface gigabitethernet	Selects a particular Gigabit Ethernet interface for configuration.
show controllers	Displays information that is specific to the hardware on a module.
show controllers fastethernet	Displays Fast Ethernet interface information, transmission statistics, and errors, and the applicable MAC destination address and VLAN filtering tables.
show controllers gigabitethernet	Displays Gigabit Ethernet interface information, transmission statistics, and errors, and the applicable MAC destination address and VLAN filtering tables.
show interfaces	Displays traffic that is seen by a specific interface.
show interfaces fastethernet	Displays information about Fast Ethernet interfaces.
show interfaces gigabitethernet	Displays information about Gigabit Ethernet interfaces.
speed	Sets the port speed for a Fast Ethernet interface.

dxi interface-dfa

To specify a map command for a point to point serial interface, use the Data Exchange Interface (dxi) command **dxiinterface-dfa** in interface configuration mode. To deletct the map command, use the **no** form of this command.

dxi interface-dfa *vpi-number vci* [{**snap** | **mux**}]
no dxi interface-dfa *vpi-number vci*

Syntax Description

vpi-number	ATM network virtual path identifier (VPI) of the permanent virtual circuit (PVC), in the range from 0 to 15. The VPI is a 4-bit field in the header of the ATM DXI frame. The VPI value is unique only on a single interface, not throughout the ATM network, because it has local significance only. Both *vpi* and *vci* cannot be specified as 0; if one is 0, the other cannot be 0.
vci	ATM network virtual channel identifier (VCI) of this PVC, in the range from 0 to 63. The VCI is a 6-bit field in the header of the ATM DXI frame. The VCI value is unique only on a single interface, not throughout the ATM network, because it has local significance only. Both *vpi* and *vci* cannot be specified as 0; if one is 0, the other cannot be 0.
snap	(Optional) LLC/SNAP encapsulation based on the protocol used in the packet. This keyword defines a PVC that can carry multiple network protocols. This is the default.
mux	(Optional) Enables multiplex (mux) encapsulation.

Command Default

No map command is specified.

Command Modes

Interface configuration

Command Default

No map definition is established.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.4	This command was integrated into Cisco IOS Release 12.4.

Examples

The following example shows how to specify a map command.

```
Router(config)# interface serial 1
Router(config-if)# dxi interface-dfa 10
```

Related Commands

Command	Description
encapsulation atm-dxi	Enables ATM-DXI encapsulation.

Command	Description
dxi pvc	Configures multiprotocol or single protocol AMT-Data Exchange Interface (dxi) encapsulation.
dxi map	Maps a protocol address to a given virtual path identifier (VPI) and virtual channel identifier (VCI).
show dxi pvc	Displays the PVC statistics for a serial interface.
smds dxi	Enables Data Exchange Interface (dxi) version 2.2 support.

dxi pvc	Configures multiprotocol or single protocol AMT-Data Exchange Interface (dxi) encapsulation.

dxs3mode

To define the controller type as an E3 or T3 controller, use the dxs3mode command in controller configuration mode. To remove the controller, use the no form of this command.

dxs3mode [{**e3** | **t3**}]
no dxs3mode [{**e3** | **t3**}]

Syntax Description

e3	(Optional) Defines an E3 controller.
t3	(Optional) Defines a T3 controller.

Command Default

t3

Command Modes

Controller configuration

Command History

Release	Modification
12.2S	This command was introduced.

Examples

The following example defines a T3 controller:

```
Router(config
)
# controller dsx3 2/0/0
Router(config
-controller)
# dsx3mode t3
```

Related Commands

Command	Description
description	Adds a description to identify particulars about a controller.

e2-clockrate

To configure serial interface 0 for E2 (8 MHz full duplex) and to shut down the other three serial interfaces (1 to 3), use the **e2-clockrate** command in interface configuration mode. To disable the full duplex E2, use the **no** form of this command.

e2-clockrate
no e2-clockrate

Syntax Description

This command has no arguments or keywords.

Command Default

All interfaces are running.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(2)XD	This command was introduced.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **e2-clockrate** command is an interface configuration command and is seen only with **interfaceserial0**. When this command is used, serial interface 0 supports speeds up to E2 (8 MHz full duplex) and the other three serial interfaces (1 to 3) are put in the "shutdown" state. Also, running this command displays the following warning message:

```
Serial interface 0 is configured to support E2 rates and serial ports "1-3" are moved to
shutdown state
.
```

Examples

The following example shows sample display output for the **e2-clockrate** EXEC command.

```
Router(config-if)#
e2-clockrate
Interface Serial 0 is configured to support clockrates up to E2 (8Mbps)
Interfaces serial 1-3 will not be operational
```

Related Commands

Command	Description
clock rate	Configures the clock rate for the hardware connections on serial interfaces such as NIMs and interface processors to an acceptable bit rate.

early-token-release

To enable early token release on Token Ring interfaces, use the **early-token-release** command in interface configuration mode. To disable this function, use the **no** form of this command.

early-token-release
no early-token-release

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Early token release is a method whereby the Token Ring interfaces can release the token back onto the ring immediately after transmitting, rather than waiting for the frame to return. This feature helps increase the total bandwidth of the Token Ring.

The Token Ring Interface Processor (TRIP) on the Cisco 7500 series routers and the Token Ring adapters on the Cisco 7200 series routers all support early token release.

Examples

The following example enables the use of early token release on Token Ring interface 1:

```
Router(config)# interface tokenring 1
Router(config-if)# early-token-release
```

The following example enables the use of early token release on the Token Ring interface processor in slot 4 on port 1 on the Cisco 7500 series routers:

```
Router(config)# interface tokenring 4/1
Router(config-if)# early-token-release
```

efm-grp

The efm-grp command is used to perform the necessary link operations (add, delete, and shutdown) of a single link after the creation of efm-bonding group. To perform the link operations in the efm-grp command, enter the config-controller-dsl-group mode. Use the no form of the command to shut down the related command.

efm-grp [{**add** | **delete** | **shutdown**}] **link** *link number*
no efm-grp [{**add** | **delete** | **shutdown**}] *link link number*

Syntax Description

link number	Designates the pairs link number.
add	Adds a link to the efm-bonding group.
delete	Deletes a link from the efm-bonding group
shutdown	Shuts down a link in the efm-bonding group.

Command Default

No default behavior or values.

Command Modes

Config-controller-dsl-group (config-controller-dsl-group)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

This command is used to add, delete, or shutdown a link in the efm-bond.

Examples

The following example shows how **efm-grp** command is used.

```
Router(config-controller-dsl-group)# efm-grp ?
add       Add a link to the EFM Bonding group
delete    Delete a link from the EFM Bonding group
shutdown  Shutdown a link in the EFM Bonding group
Router(config-controller-dsl-group)# efm-grp add ?
link  EFM Bonding group link configuration

Router(config-controller-dsl-group)# efm-grp add link ?
<0-3>  Link pair number
```

Related Commands

Command	Description
controller shdsl	Configures a controller for SHDSL mode and enters config-controller mode.
shdsl annex	Defines the SHDSL G.991.2 standard.
shdsl rate	Defines the SHDSL rate.
show controller shdsl	Displays the status of the controller that is configured for SHDSL mode.

eigrp interface

Note Effective with Cisco IOS Release 15.0(1)M, the **eigrp interface**command is replaced by the **dampening-change** command and the **dampening-interval** command. See the **dampening-change** and **dampening-interval**commands for more information.

To set a threshold value to minimize hysteresis in a router-to-radio configuration, use the **eigrp interface** command in interface configuration mode. To reset the hysteresis threshold to the default value, use the **no** form of this command.

eigrp *vmi-interface-number* **interface** [**dampening-change** *value*] [**dampening-interval** *value*]
no eigrp *vmi-interface-number* **interface** [**dampening-change** *value*] [**dampening-interval** *value*]

Syntax Description

vmi-interface-number	The number assigned to the VMI interface.
dampening-change *value*	(Optional) Value used to minimize the effect of frequent routing changes in router-to-radio configurations. Percent interface metric must change to cause update. Value range is 1 to 100.
dampening-interval *value*	(Optional) Specifies the time interval in seconds to check the interface metrics at which advertising of routing changes occurs. The default value is 30 seconds. Value range is 1 to 65535.

Command Default

Default for change-based dampening is 50 percent of the computed metric.

Default for interval-based dampening is 30 seconds.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(15)XF	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.
15.0(1)M	This command was replaced. This command was replaced by the **dampening-change**command and the **dampening-interval** command.

Usage Guidelines

This command advertises routing changes for EIGRP traffic only.

The REPLY sent to any QUERY will always contain the latest metric information. Exceptions which will result in immediate UPDATE being sent:

- A down interface
- A down route
- Any change in metric which results in the router selecting a new next hop

Change-based Dampening

The default value for the change tolerance will be 50% of the computed metric. It can be configured in the range from 0 to 100 percent. If the metric change of the interface is not greater (or less) than the current metric plus or minus the specified amount, the change will not result in a routing change, and no update will be sent to other adjacencies.

Interval-based Dampening

The default value for the update intervals is 30 seconds. It can be configured in the range from 0 to 64535 seconds. If this option is specified, changes in routes learned though this interface, or in the interface metrics, will not be advertised to adjacencies until the specified interval is met. When the timer expires, any changes detected in any routes learned through the interface, or the metric reported by the interfaces will be sent out.

Examples

Change-based Dampening Example

The following example sets the threshold to 50 percent tolerance routing updates involving VMI interfaces and peers:

```
interface vmi1
 ip address 10.2.2.1 255.255.255.0
 ipv6 address 2001:0DB1:2::1/96
 ipv6 enable
 eigrp 1 interface dampening-change 50
 physical-interface Ethernet0/0
```

Interval-based Dampening Example

The following example sets the interval to 30 seconds at which updates occur for topology changes that affect VMI interfaces and peers:

```
interface vmi1
 ip address 10.2.2.1 255.255.255.0
 ipv6 address 2001:0DB1:2::1/96
 ipv6 enable
 eigrp 1 interface dampening-interval 30
 physical-interface Ethernet0/0
```

Related Commands

Command	Description
debug vmi	Displays debugging output for virtual multipoint interfaces (VMIs)
interface vmi	Creates a virtual multipoint interface (VMI) that can be configured and applied dynamically.

emulation-mode

To configure Configuration Circuit Emulation (CEM), use the emulation-mode command in unidirectional mode.

emulation-mode {**bidirectional** | **unidirectional** {**rx** | **tx**}}
no emulation-mode

Syntax Description

rx	When the CEM is in rx-only mode, there is no data transmitted by that CEM. The CEM status shows "active (rx-only)".
tx	The CEM in tx-only mode does not receive any data. There is no data sent to the IP side and the received data is silently dropped at the CEM. The CEM status shows "active (tx-only)".

Command Default

Default mode is unidirectional mode.

Command Modes

Configuration CEM mode (emulation-mode).

Command History

Release	Modification
12.4(20)YA	This command was introduced.

Usage Guidelines

You can use the emulation-mode command to configure the CEM in unidirectional mode. Once configured, traffic will flow only in that direction through the CEM channel. The CEM status will show as "active (rx-only)" or "active (tx-only)" depending on the configuration. To disable the command's effect, use the **no** form of this command.

Examples

The following example shows how the command configures the traffic in unidirectional mode:

```
Router(config-cem
)# emulation-mode unidirectional tx
```

The following example shows how the command configures the traffic in bidirectional mode:

```
Router(config-cem
)# emulation-mode bidirectional
```

encapsulation

To set the encapsulation method used by the interface, use the **encapsulation** command in interface configuration mode. To remove the encapsulation, use the **no** form of this command.

encapsulation *encapsulation-type*
no encapsulation *encapsulation-type*

Syntax Description

encapsulation-type	Encapsulation type; one of the following keywords: • **atm-dxi** -- ATM Mode-Data Exchange Interface. • **bstun** --Block Serial Tunnel. • **dot1q** *vlan-id* [**native**]--Enables IEEE 802.1q encapsulation of traffic on a specified subinterface in VLANs. The *vlan-id* argument is a virtual LAN identifier. The valid range is from 1 to 1000. The optional **native** keyword sets the PVID value of the port to the *vlan-id* value. • **frame-relay** --Frame Relay (for serial interface). • **hdlc** -- High-Level Data Link Control (HDLC) protocol for serial interface. This encapsulation method provides the synchronous framing and error detection functions of HDLC without windowing or retransmission. This is the default for synchronous serial interfaces. • **isl** *vlan-id* --Inter-Switch Link (ISL) (for VLANs). • **lapb** --X.25 Link Access Procedure, Balanced. Data link layer protocol (LAPB) DTE operation (for serial interface). • **ppp** -- PPP (for serial interface). • **sde** *said* --IEEE 802.10. The *said* argument is a security association identifier. This value is used as the VLAN identifier. The valid range is from 0 to 0xFFFFFFFE. • **sdlc** --IBM serial Systems Network Architecture (SNA). • **sdlc-primary** --IBM serial SNA (for primary serial interface) . • **sdlc-secondary** --IBM serial SNA (for secondary serial interface). • **slip** --Specifies Serial Line Internet Protocol (SLIP) encapsulation for an interface configured for dedicated asynchronous mode or dial-on-demand routing (DDR). This is the default for asynchronous interfaces. • **smds** --Switched Multimegabit Data Services (SMDS) (for serial interface). • **ss7** --Sets the encapsulation type to SS7 and overrides the serial interface objects high-level data link control (HDLC) default.

Command Default

The default depends on the type of interface. For example, synchronous serial interfaces default to HDLC and asynchronous interfaces default to SLIP.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
10.3	The **sde** keyword was added to support IEEE 802.10
11.1	The **isl** keyword was added to support the Interswitch Link (ISL) Cisco protocol for interconnecting multiple switches and routers, and for defining virtual LAN (VLAN) topologies.
11.3(4)T	The **tr-isltrbrf-vla**n keyword was added to support TRISL, a Cisco proprietary protocol for interconnecting multiple routers and switches and maintaining VLAN information as traffic goes between switches.
12.0(1)T	The **dot1q** keyword was added to support IEEE 8021q standard for encapsulation of traffic on a specified subinterface in VLANs.
12.1(3)T	The **native** keyword was added.
12.2(11)T	This command was modified to include the **ss7** keyword in support of integrated signaling link terminal capabilities.
12.2(13)T	Support for IPv6 was added.
12.3(2)T	The **tr-isltrbrf-vla**n keyword was removed because support for the TRISL protocol is no longer available in Cisco IOS software.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.5	This command was updated. It was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

SLIP and PPP

To use SLIP or PPP, the router or access server must be configured with an IP routing protocol or with the **iphost-routing** command. This configuration is done automatically if you are using old-style **slipaddress** commands. However, you must configure it manually if you configure SLIP or PPP via the **interfaceasync** command.

On lines configured for interactive use, encapsulation is selected by the user when they establish a connection with the **slip** or **ppp** EXEC command.

IP Control Protocol (IPCP) is the part of PPP that brings up and configures IP links. After devices at both ends of a connection communicate and bring up PPP, they bring up the control protocol for each network protocol that they intend to run over the PPP link such as IP or IPX. If you have problems passing IP packets and the **showinterface** command shows that line is up, usethe**negotiations** command to see if and where the negotiations are failing. You might have different versions of software running, or different versions of PPP, in which case you might need to upgrade your software or turn off PPP option negotiations. All IPCP options as listed in RFC 1332, *PPP Internet Protocol Control Protocol (IPCP)* , are supported on asynchronous lines. Only Option 2, TCP/IP header compression, is supported on synchronous interfaces.

PPP echo requests are used as keepalive packets to detect line failure. The **nokeepalive** command can be used to disable echo requests. For more information about the **nokeepalive** command, refer to the chapter “IP Services Commands” in the *CiscoIOSIPCommandReference,Volume1of4:AddressingandServices*and to thechapter“Configuring IP Services” in the *CiscoIOSIPConfigurationGuide*.

To use SLIP or PPP, the Cisco IOS software must be configured with an IP routing protocol or with the **iphost-routing** command. This configuration is done automatically if you are using old-style **slipaddress** commands. However, you must configure it manually if you configure SLIP or PPP via the **interfaceasync** command.

Note Disable software flow control on SLIP and PPP lines before using the **encapsulation** command.

SS7

The SS7 encapsulation command is new with the Integrated SLT feature and is available only for interface serial objects created by the channel-group command. For network access server (NAS) platforms, the encapsulation for channel group serial interface objects defaults to HDLC. You must explicitly set the encapsulation type to SS7 to override this default.

When encapsulation is set to SS7, the encapsulation command for that object is no longer available. A serial SS7 link is deleted only when its associated dial feature card (DFC) card is removed. As with existing Cisco 26xx-based SLTs, you do not need to specify whether the SS7 link is to be used as an A-link or an F-link.

By itself this command does not select the correct encapsulation type. Therefore, once created, you must set the encapsulation type to the new SS7 value, as well as assign a session channel ID to the link at the serial interface command level. The configuration on a digital SS7 link can be saved (no shutdown) only when its encapsulation is successfully set to SS7 and it has been assigned a channel identifier.

VLANs

Do not configure encapsulation on the native VLAN of an IEEE 802.1q trunk without the **native** keyword. (Always use the **native** keyword when the *vlan-id* is the ID of the IEEE 802.1q native VLAN.)

For detailed information on use of this command with VLANs, refer to the *Cisco IOS Switching Services Configuration Guide* and the *Cisco IOS Switching Services Command Reference* .

Examples

The following example shows how to reset HDLC serial encapsulation on serial interface 1:

```
Router(config)# interface serial 1
Router(config-if)# encapsulation hdlc
```

The following example shows how to enable PPP encapsulation on serial interface 0:

```
Router(config)# interface serial 0
Router(config-if)# encapsulation ppp
```

The following example shows how to configure async interface 1 for PPP encapsulation:

```
Router(config)# interface async 1
Router(config-if)# encapsulation ppp
```

To learn more about the virtual serial interface and check SS7 encapsulation, enter the show interfaces serial *slot/trunk:channel-group* command in privileged EXEC mode, as in the following example:

```
Router# show interfaces serial 7/3:1
Serial7/3:1 is up, line protocol is down
 Hardware is PowerQUICC Serial
 MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
  reliability 255/255, txload 4/255, rxload 1/255
 Encapsulation SS7 MTP2, loopback not set
 Keepalive set (10 sec)
 Last input never, output 00:00:00, output hang never
 Last clearing of "show interface" counters 03:53:40
 Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 26000 bits/sec, 836 packets/sec
  0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  11580159 packets output, 46320636 bytes, 0 underruns
  0 output errors, 0 collisions, 1 interface resets
  0 output buffer failures, 0 output buffers swapped out
  2 carrier transitions
  DCD=up DSR=down DTR=down RTS=down CTS=down
```

Related Commands

Command	Description
channel-group	Assigns a channel group and selects the DSO time slots desired for SS7 links.
encapsulation x25	Specifies operation of a serial interface as an X.25 device.
keepalive	Sets the keepalive timer for a specific interface.
ppp	Starts an asynchronous connection using PPP.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
ppp bap call	Sets PPP BACP call parameters.
slip	Starts a serial connection to a remote host using SLIP.

end (satellite initial configuration)

To exit satellite initial configuration mode, save any new or changed parameters, and reset the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT), use the **end** command in satellite initial configuration mode.

end

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Satellite initial configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The **end** command is identical to the **exit** command in satellite initial configuration mode.

When you enter the **exit** or **end** command to exit satellite initial configuration mode, the system automatically saves any changed parameters to the NM-1VSAT-GILAT network module nonvolatile memory and resets the NM-1VSAT-GILAT network module.

Examples

The following example shows what appears when you enter the **end** or **exit**command after changing one or more initial configuration parameters:

```
Router(sat-init-config)# end

Applying changed parameters to the satellite module.
Parameter update succeeded.  Module is now resetting.
Router#
```

The following example shows what appears when you enter the **end** or **exit** command when no parameters have been changed:

```
Router(sat-init-config)# end

Router#
```

Related Commands

Command	Description
apply	Saves new or changed satellite initial configuration parameters and resets the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT).
exit (satellite initial configuration)	Exits satellite initial configuration mode, saves any new or changed parameters, and resets the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT).

equipment loopback

To run loopbacks in conjunction with remote equipment, use the **equipmentloopback**command in controller configuration mode. To terminate the loopback, use the no form of this command.

equipment [{**customer** | **network**}] **loopback**
no **equipment** [{**customer** | **network**}] **loopback**

Syntax Description

customer	(Optional) Enables the line card to respond to remote T3 loopback commands from the remote T3 equipment.
network	(Optional) Causes the line card to ignore remote T3 loopback commands.

Command Default

No default behavior or values.

Command Modes

Controller configuration

Command History

Release	Modification
12.2S	This command was introduced

Examples

The following example configures an equipment network loopback:

```
Router(config
)
# controller t3 1/0/0
Router(config
-controller)
# equipment network loopback
```

Related Commands

Command	Description
loopback	Enables controller loopbacks.

errdisable detect cause

To enable error-disable detection, use the **errdisable detect cause** command in global configuration mode. To disable error-disable detection, use the **no** form of this command.

errdisable detect cause {**all** | **bpduguard** | **dtp-flap** | **l2ptguard** | **link-flap** | **packet-buffer-error** | **pagp-flap** | **rootguard** | **udld**}
no errdisable detect cause {**all** | **bpduguard** | **dtp-flap** | **l2ptguard** | **link-flap** | **pagp-flap** | **rootguard** | **udld**}

Syntax Description

all	Specifies error-disable detection for all error-disable causes.
bpduguard	Specifies detection for the Bridge Protocol Data Unit (BPDU)-guard error-disable cause.
dtp-flap	Specifies detection for the Dynamic Trunking Protocol (DTP)-flap error-disable cause.
l2ptguard	Specifies detection for the Layer 2 Protocol Tunneling guard error-disable cause.
link-flap	Specifies detection for the link flap error-disable cause.
packet-buffer-error	Causes the packet buffer error to error-disable the affected port.
pagp-flap	Specifies detection for the Port Aggregation Protocol (PAgP)-flap error-disable cause.
rootguard	Specifies detection for the root-guard error-disable cause.
udld	Specifies detection for the Unidirectional Link Detection (UDLD) error-disable cause.

Command Default

Error-disable detection is enabled for all causes.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(14)SX	This command was modified. Support was added for the Supervisor Engine 720.
12.2(17b)SXA	This command was modified. The **packet-buffer-error** keyword was added.
12.2(17d)SXB	This command was modified. Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

> **Note** Entering the **no errdisable detect cause packet-buffer-error** command allows you to detect the fault that triggers a power cycle of the affected module.

A cause (bpduguard, dtp-flap, link-flap, pagp-flap, root-guard, udld) is defined as the reason why the error-disable state occurred. When a cause is detected on an interface, the interface is placed in an error-disable state (an operational state that is similiar to the link-down state).

You must enter the **shutdown** and then the **no shutdown** commands to recover an interface manually from the error-disable state.

Examples

The following example shows how to enable error-disable detection for the Layer 2 protocol-tunnel guard error-disable cause:

```
Router(config)#
errdisable detect cause l2ptguard
```

Related Commands

Command	Description
show errdisable detect	Displays the error-disable detection status.
show interfaces status	Displays the interface status or a list of interfaces in an error-disable state on LAN ports only.
shutdown	Disables an interface.

errdisable recovery

To configure recovery mechanism variables, use the **errdisable recovery** command in global configuration mode. To return to the default state, use the **no** form of this command.

errdisable recovery {**cause** {**all** | **arp-inspection** | **bpduguard** | **channel-misconfig** | **dhcp-rate-limit** | **dtp-flap** | **gbic-invalid** | **l2ptguard** | **link-flap** | **pagp-flap** | **psecure-violation** | **security-violation** | **rootguard** | **udld** | **unicast-flood**} | **interval** *seconds*}
no errdisable recovery {**cause** {**all** | **arp-inspection** | **bpduguard** | **channel-misconfig** | **dhcp-rate-limit** | **dtp-flap** | **gbic-invalid** | **l2ptguard** | **link-flap** | **pagp-flap** | **psecure-violation** | **security-violation** | **rootguard** | **udld** | **unicast-flood**} | **interval** *seconds*}

Syntax Description

cause	Enables error-disable recovery from a specific cause.
all	Enables the recovery timers for all error-disable causes.
arp-inspection	Enables error-disable recovery from an Address Resolution Protocol (ARP) inspection cause.
bpduguard	Enables the recovery timer for the Bridge Protocol Data Unit (BPDU)-guard error-disable cause.
channel-misconfig	Enables the recovery timer for the channel-misconfig error-disable cause.
dhcp-rate-limit	Enables the recovery timer for the Dynamic Host Configuration Protocol (DHCP)-rate-limit error-disable cause.
dtp-flap	Enables the recovery timer for the Dynamic Trunking Protocol (DTP)-flap error-disable cause.
gbic-invalid	Enables the recovery timer for the Gigabit Interface Converter (GBIC)-invalid error-disable cause.
l2ptguard	Enables the recovery timer for the Layer 2 Protocol Tunneling (L2PT) error-disable cause.
link-flap	Enables the recovery timer for the link-flap error-disable cause.
pagp-flap	Enables the recovery timer for the Port Aggregation Protocol (PAgP)-flap error-disable cause.
psecure-violation	Enables the recovery timer for the psecure-violation error-disable cause.
security-violation	Enables the automatic recovery of ports that were disabled because of 802.1X security violations.
rootguard	Enables the recovery timer for the root-guard error-disable cause.
udld	Enables the recovery timer for the Unidirectional Link Detection (UDLD) error-disable cause.
unicast-flood	Enables the recovery timer for the unicast-flood error-disable cause.

interval *seconds*	Specifies the time, in seconds, to recover from a specified error-disable cause. The range is from 30 to 86400. The default interval is 300.

Command Default

The recovery mechanisms are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(14)SX	This command was modified. This command was implemented on the Supervisor Engine 720.
12.2(17d)SXB	This command was modified. This command was implemented on the Supervisor Engine 2.
12.2(18)SXD	This command was modified. The **arp-inspection** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

A cause (bpduguard, channel-misconfig, dhcp-rate-limit, dtp-flap, l2ptguard, link-flap, pagp-flap, psecure-violation, security-violation, rootguard, udld, or unicast-flood) is defined as the reason why the error-disable state occurred. When a cause is detected on an interface, the interface is placed in an error-disable state (an operational state that is similar to the link-down state). If you do not enable error-disable recovery for the cause, the interface stays in the error-disable state until a shutdown and no shutdown occur. If you enable recovery for a cause, the interface is brought out of the error-disable state and allowed to retry operation once all the causes have timed out.

You must enter the **shutdown** command and then the **no shutdown** command to manually recover an interface from the error-disable state.

Note A separate line is required each time you want to enter the **errdisable recovery cause** command to add a new reason for recovery; each new reason does not get appended to the original single line. This means you must enter each new reason separately.

Examples

This example shows how to enable the recovery timer for the BPDU-guard error-disable cause:

```
Router(config)#
 errdisable recovery cause bpduguard
```

This example shows how to set the recovery timer to 300 seconds:

```
Router(config)#
 errdisable recovery interval 300
```

Related Commands

Command	Description
show errdisable recovery	Displays the information about the error-disable recovery timer.
show interfaces status	Displays the interface status or a list of interfaces in an error-disabled state on LAN ports only.
shutdown	Disables an interface.

error throttling

To stop receiving error data packets on multiple channel groups configured on all interfaces on the T1 controller of a channelized T3 port adapter or on the E1 controller of a channelized E3 port adapter, use the **errorthrottling** command in controller configuration mode. To continue receiving error data packets on all channels on the T1 or E1 controller, use the no form of this command.

error throttling
no error throttling

Syntax Description

This command has no arguments or keywords.

Command Default

The **errorthrottling** command is enabled by default on a T3 or a E3 port adapter.

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
12.2(19c)	This command was introduced.
15.0(1)M3	This command was modified. This command can be enabled on E1 controllers.
12.2(33)SRD5	This command was integrated into Cisco IOS Release 12.2(33)SRD5.

Usage Guidelines

Use the **showcontrollerst3** command or **showcontrollerse3** command to display whether the current router configuration has error throttling enabled or disabled.

The **errorthrottling** command disables the T1 or E1 level clock in order to stop receiving error data packets on a T1 or E1 controller.

When a T1 or a E1 has multiple channel groups configured over it, error throttling affects all the channels on a T1 or a E1. If any single interface receives a burst of errors, over a short duration, such as 400 errors in 100 milliseconds (ms), the T1 or E1 clock is turned off for a period of 100 ms. When there is a high rate of errors, the error rate is likely to continue for a long duration of time. Using error throttling to stop receiving the error data packets reduces wasteful processing and discarding of error packets.

The **noerrorthrottling** command allows all the error data packets to be processed, dropped, and accounted for on a T1 or a E1 controller. When the error rate is high, the CPU can become overloaded.

When the **noerrorthrottling** command is used to configure a T3 or a E3 port, the configuration applies to all of the 28 associated T1 or E1 channels.

Examples

The following example enables error throttling by disabling the T1 clock in order to stop receiving error data packets on a T1 controller:

```
Router(config-controller)# error throttling
```

The following example uses the **showcontrollerst3** command to display partial output showing that error throttling is enabled on the T1 controller:

```
Router# show controllers t3 2/1/0
```

```
T3 2/1/0 is down.  Hardware is 2CT3 single wide port adapter
  CT3 H/W Version: 0.2.2, CT3 ROM Version: 1.0, CT3 F/W Version: 2.5.1
  FREEDM version: 1, reset 0 resurrect 0
  Applique type is Channelized T3
  Transmitter is sending remote alarm.
  Receiver has loss of signal.
  FEAC code received: No code is being received
  Framing is M23, Line Code is B3ZS, Clock Source is Internal
  Rx-error throttling on T1's ENABLED
  .
```

The following example uses the **showcontrollerse3** command to display partial output showing that error throttling is enabled on the E1 controller:

```
Router# show controller e3 5/0
*Mar 14 21:19:06.795: %SYS-5-CONFIG_I: Configured from console by console
E3 5/0 is up.
  CE3 H/W Version : 3.1.0, CE3 ROM Version : 1.1, CE3 F/W Version : 1.2.1
  Applique type is Channelized E3
  Total available channels 128, used 4
  No alarms detected. Line Code is HDB3, Clock Source is Line.
  Rx-error throttling on E1's ENABLED
  Data in current interval (564 seconds elapsed):
     0 Line Code Violations, 0 P-bit Coding Violation
     0 C-bit Coding Violation
     0 P-bit Err Secs, 0 P-bit Severely Err Secs
     0 Severely Err Framing Secs, 0 Unavailable Secs
     0 Line Errored Secs, 0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
E3 5/0 E1 1
  No alarms detected.
  Framing is crc4, Clock Source is line, National bits are 0x1F.
  Data in current interval (565 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
     0 Unavail Secs
E3 5/0 E1 2
  No alarms detected.
  Framing is crc4, Clock Source is line, National bits are 0x1F.
```

Related Commands

Command	Description
show controllers e3	Displays information about E3 links, and displays hardware and software driver information for the E3 controller.
show controllers t3	Displays information about T3 links, and displays hardware and software driver information for the T3 controller.

esmc mode ql-disabled

To disable the Ethernet synchronization message channel (ESMC) on an interface, use the **esmc mode ql-disabled**command in interface configuration mode. To remove the quality level (QL) disabled mode and get back to the default ql-enabled mode, use the **no** form of this command.

esmc mode ql-disabled
no esmc mode ql-disabled

Syntax Description

This command has no arguments or keywords.

Command Default

The ESMC mode is ql-enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.0(1)S	This command was introduced.
15.1(2) SNI	This command was introduced in Cisco ASR 901 Aggregation Services Router.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

You can use the **esmc modeql-disabled** command only if a synchronous Ethernet (SyncE) capable interface is installed on the device. When this command is used no QL ESMC packets are sent during network clock synchronization.

Examples

The following example shows how to enable ESMC process:

```
Device(config-if)# esmc mode ql-disabled
```

Related Commands

Command	Description
esmc process	Enables the ESMC process in a device.
show esmc	Displays the enabled ESMCs in a device.
show interfaces accounting	Displays the number of packets of each protocol type that have been sent through all configured interfaces.

esmc process

To enable the Ethernet synchronization message channel (ESMC) process in a router, use the **esmc process**command in global configuration mode. To disable the process, use the **no** form of this command.

esmc process
no esmc process

Syntax Description

This command has no arguments or keywords.

Command Default

The ESMC process is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)S	This command was introduced.
15.1(2) SNI	This command was introduced in Cisco ASR 901 Aggregation Services Router.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

You can use the **esmc process** command only if a synchronous Ethernet (SyncE) capable interface is installed on the device. ESMC is the communication channel for conveying clock information in SyncE. You can use the ESMC process in a SyncE to synchronize the clock frequency over an Ethernet port.

Examples

The following example shows how to enable ESMC process:

```
Device(config)# esmc process
```

Related Commands

Command	Description
esmc mode ql-disabled	Disables the ESMC on an interface.
show esmc	Displays the enabled ESMCs in a device.
show interfaces accounting	Displays the number of packets of each protocol type that have been sent through all configured interfaces.

exit (satellite initial configuration)

To exit satellite initial configuration mode, save any new or changed parameters, and reset the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT), use the **exit** command in satellite initial configuration mode.

exit

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Satellite initial configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The **exit**command is identical to the **end** command in satellite initial configuration mode.

When you enter the **exit** or **end** command to exit satellite initial configuration mode, the system automatically saves any changed parameters to the NM-1VSAT-GILAT network module nonvolatile memory and resets the NM-1VSAT-GILAT network module.

Examples

The following example shows what appears when you enter the **exit** or **end**command after changing one or more initial configuration parameters:

```
Router(sat-init-config)# exit

Applying changed parameters to the satellite module.
Parameter update succeeded.  Module is now resetting.
Router#
```

The following example shows what appears when you enter the **exit** or **end**command when no parameters have been changed:

```
Router(sat-init-config)# exit

Router#
```

Related Commands

Command	Description
apply	Saves new or changed satellite initial configuration parameters and resets the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT).
end (satellite initial configuration)	Exits satellite initial configuration mode, saves any new or changed parameters, and resets the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT).

F through H

fabric buffer-reserve

To reserve ASIC buffers, use the **fabricbuffer-reserve** command. in global configuration mode. To return to the default settings, use the **no** form of this command.

fabric buffer-reserve [{**high** | **low** | **medium***value*}]
[**default**] **fabric buffer-reserve queue**
no fabric buffer-reserve

Syntax Description

high	(Optional) Reserves the high (0x5050) ASIC buffer spaces.
low	(Optional) Reserves the low (0x3030) ASIC buffer spaces.
medium	(Optional) Reserves the medium (0x4040) ASIC buffer spaces.
value	(Optional) 16-bit value; valid values are from 0x0 to 0x5050.
default	(Optional) Specifies the default queue setting.
queue	Specifies the queue setting for the buffer reserve.

Command Default

The default settings are as follows:

- Buffer reserve is set to 0x0.
- Two queues.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(18)SXF	This command was changed to add the **queue** keyword.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Note Use this command only under the direction of Cisco TAC.

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 32.

The **fabricbuffer-reservequeue**command is supported on Cisco 7600 series routers that are configured with the following modules:

- WS-X6748-GE-TX
- WS-X6724-SFP

- WS-X6748-SFP
- WS-X6704-10GE

Entering the **defaultfabricbuffer-reservequeue** command is the same as entering the **fabricbuffer-reservequeue** command.

You can enter the **fabricbuffer-reserve** command to improve the system throughput by reserving ASIC buffers.

This command is supported on the following modules:

- WS-X6704-10GE
- WS-X6748-SFP
- WS-X6748-GE-TX
- WS-X6724-SFP

Examples

This example shows how to reserve the high (0x5050) ASIC buffer spaces:

```
Router(config)# fabric buffer-reserve high
Router(config)#
```

This example shows how to reserve the low (0x3030) ASIC buffer spaces:

```
Router(config)# fabric buffer-reserve low
Router(config)#
```

fabric clear-block

To enable the clear-block congestion control for the fabric channels, use the **fabricclear-block** command in global configuration mode. To disable the clear-block congestion control for the fabric channels, use the **no** form of this command.

fabric clear-block
no fabric clear-block

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(17d)SXB1	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Note Do not enter the **fabricclear-block**command unless TAC advises you to do so.

This command is supported only with Supervisor Engine 720 hardware revision 4.0 and later releases.

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 32.

Examples

This example shows how to enable the clear-block congestion control for the fabric channels:

```
Router(config)# fabric clear-block
Router(config)#
```

This example shows how to disable the clear-block congestion control for the fabric channels:

```
Router(config)# no fabric clear-block
Router(config)#
```

fabric error-recovery fabric-switchover (virtual switch)

To enable a supervisor engine switchover when excessive fabric synchronization errors are detected on the fabric-enabled module, use the **fabricerror-recoveryfabric-switchover** command in global configuration mode. To disable the supervisor engine switchover for excessive fabric synchronization errors, use the **no** form of this command.

fabric switch *num* **error-recovery fabric-switchover**
no fabric switch *num* **error-recovery fabric-switchover**

Syntax Description

switch *num*	Specifies the switch number; valid values are 1 and 2.

Command Default

Excessive fabric synchronization errors initiate a supervisor engine switchover, and the configuration is not saved to the configuration file.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXH1	Support for this command was introduced.

Usage Guidelines

When a fabric-capable switching module has fabric errors, a supervisor engine switchover is initiated.

You can use the **nofabricerror-recoveryfabric-switchover** command to avoid the supervisor engine switchover. This command does not perform the supervisor engine switchover but powers down the module that is experiencing the excessive fabric errors. This command is saved to the configuration file.

Examples

The following example shows how to enable a supervisor engine switchover when excessive fabric synchronization errors are detected on the fabric-enabled module:

```
Router(config)# fabric switch 2 error-recovery fabric-switchover
Router(config)#
```

The following example shows how to disable a supervisor engine switchover when excessive fabric synchronization errors are detected on the fabric-enabled module:

```
Router(config)# no fabric switch 2 error-recovery fabric-switchover
Router(config)#
```

Related Commands

Command	Description
show fabric	Displays the information about the crossbar fabric .

fabric lcd-banner

To specify the message-of-the-day (MOTD) banner for display on the Switch Fabric Module, use the **fabriclcd-banner** command in global configuration mode. To delete the MOTD banner, use the **no** form of this command.

fabric lcd-banner *d message d*
no fabric lcd-banner

Syntax Description

d	Delimiting character; see the "Usage Guidelines" section for additional guidelines.
message	Message text; see the "Usage Guidelines" section for additional guidelines.

Command Default

No MOTD banner is specified.

Command Modes

Global configuration

Command History

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2 only.

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 32

You cannot use the delimiting character in the banner message. The delimiter is a character of your choice--a pound sign (#), for example.

You can replace tokens with the corresponding configuration argument.

Follow this command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.

This MOTD banner is useful for displaying messages that affect all users (such as impending system shutdowns).

When you connect to the router, the MOTD banner appears before the login prompt. After you successfully log in to the router, the EXEC banner or incoming banner is displayed, depending on the type of connection. For a reverse Telnet login, the incoming banner is displayed. For all other connections, the router displays the EXEC banner.

To customize the banner, use tokens in the form $(token) in the message text. Tokens display current Cisco IOS configuration arguments, such as the router's hostname and IP address.

The table below describes the command tokens.

Table 14: Command Tokens

Token	Information Displayed in the Banner
$(hostname)	Displays the router's hostname.

$(domain)	Displays the router's domain name.
$(line)	Displays the VTY or TTY (async) line number.
$(line-desc)	Displays the description that is attached to the line.

Examples

This example shows how to set a MOTD banner for display on the Switch Fabric Module LCD display; the pound sign (#) is used as a delimiting character:

```
Router(config)# fabric lcd-banner#
Building power will be off from 7:00 AM until 9:00 AM this coming Tuesday.
#
```

This example shows how to set a MOTD banner; the percent sign (%) is used as a delimiting character:

```
Router(config)# fabric lcd-banner%
Enter TEXT message.  End with the character '%'.
You have entered $(hostname).$(domain) on line $(line) ($(line-desc)) %
```

When the MOTD banner is executed, you see the following (notice that the $(token) syntax is replaced by the corresponding configuration argument):

```
You have entered company.ourdomain.com on line 5 (Dialin Modem)
```

Related Commands

Command	Description
banner exec	Specifies and enables a message to be displayed when an EXEC process is created.
banner incoming	Defines and enables a banner to be displayed when there is an incoming connection to a terminal line from a host on the network.
banner login	Defines and enables a customized banner to be displayed before the username and password login prompts.
banner slip-ppp	Allows customization of the banner that is displayed when a SLIP or PPP connection is made.
exec-banner	Reenables the display of EXEC and MOTD banners on the specified line or lines.
motd-banner	Enables the display of MOTD banners on the specified line or lines.

fabric required

To prevent the Cisco 7600 series routers from coming online without a Switch Fabric Module, use the **fabricrequired**command in global configuration mode. To allow the Cisco 7600 series routers to come up without a Switch Fabric Module, use the **no** form of this command.

fabric required
no fabric required

Syntax Description

This command has no arguments or keywords.

Command Default

A Switch Fabric Module is not required.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 32.

If you enter the **fabricrequired** command, when you remove or power down the last Switch Fabric Module, all modules except the supervisor engine, power down. When you insert or power on the first Switch Fabric Module, the modules that were previously powered down power up if the Switch Fabric Module configuration is not in conflict with other configurations.

If you enter the **nofabricrequired** command, the modules will also power on if a Switch Fabric Module is not present and the configuration allows for it.

Examples

This example shows how to prevent the Cisco 7600 series routers from coming online without a Switch Fabric Module:

```
Router(config)#
fabric required
Router(config)#
```

This example shows how to allow the Cisco 7600 series routers to come up without a Switch Fabric Module:

```
Router(config)#
no fabric required
Router(config)#
```

Related Commands

Command	Description
show fabric	Displays the information about the crossbar fabric.

fabric switching-mode allow

To enable various switching modes in the presence of two or more fabric-enabled switching modules, use the **fabricswitching-modeallow** command in global configuration mode. To disable the settings, use the **no** form of this command.

fabric switching-mode allow {**bus-mode** | **dcef-only** | **truncated** [**threshold** [*mod*]]}
no fabric switching-mode allow {**bus-mode** | **truncated** [**threshold**]}

Syntax Description

bus-mode	Specifies a module to run in bus mode.
dcef-only	Allows switching in distributed Cisco Express Forwarding (dCEF)-only mode.
truncated	Specifies a module to run in truncated mode.
threshold *mod*	(Optional) Specifies the number of fabric-enabled modules for truncated switching mode; see the "Usage Guidelines" section for additional information.

Command Default

The truncated mode is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	This command was modified. This command supports the Supervisor Engine 2.
12.2(18)SXD1	This command was modified. The **dcef-only** keyword was added on the Supervisor Engine 2.
12.2(18)SXE	This command was modified. Support for OIR performance enhancement and the **dcef-only** keyword was added on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was modified. This command was introduced on the Supervisor Engine 720-10GE.

Usage Guidelines

This command is not supported on Catalyst 6500 or Cisco 7600 series routers that are configured with a Supervisor Engine 32.

Ethernet ports are not disabled when this command is entered on a Supervisor Engine 720-10GE. This command is also supported with Supervisor Engine 720 starting with Release 12.2(33)SXI2. However, prior to Release 12.2(33)SXI2, if all the installed switching modules have Distributed Forwarding Cards (DFCs), enter the **fabricswitching-modeallowdcef-only** command to disable the Ethernet ports on both supervisor engines. Entering this command ensures that all modules are operating in dCEF-only mode and simplifies switchover to the redundant supervisor engine.

With a Supervisor Engine 2 and Release 12.2(18)SXD1 and later releases, if all the installed switching modules have DFCs, enter the **fabricswitching-modeallowdcef-only** command to disable the Ethernet ports on the redundant supervisor engine. Entering this command ensures that all modules are operating in dCEF-only mode.

Note The **fabricswitching-modeallowdcef-only** command is accepted only in stateful switchover (SSO) redundancy mode.

Bus mode--Supervisor engines use this mode for traffic between nonfabric-enabled modules and for traffic between a nonfabric-enabled module and a fabric-enabled module. In this mode, all traffic passes between the local bus and the supervisor engine bus.

dCEF-only--Supervisor engines, both active and redundant, operate as nonfabric-capable modules with their uplink ports relying on the Policy Feature Card (PFC) on the active supervisor engine for all forwarding decisions. For the Supervisor 720-10G, the uplink ports on both the active and standby routers will remain active. If all other modules are operating in dCEF-only mode, module Online Insertion and Removal (OIR) is nondisruptive.

Note The system message “PSTBY-2-CHUNKPARTIAL: Attempted to destroy partially full chunk, chunk 0xB263638, chunk name: MET FREE POOL” is displayed on the Supervisor Engine if both the **fabricswitching-modeallowdcef-only** and **ipv6mfibhardware-switchinguplink** commands are configured. The router will ignore the command configured last.

Truncated mode--Supervisor engines use this mode for traffic between fabric-enabled modules when there are both fabric-enabled and nonfabric-enabled modules installed. In this mode, line cards send a truncated version of the traffic (the first 64 bytes of the frame) over the Catalyst bus.

Compact mode--Supervisor engines use this mode for all traffic when only fabric-enabled modules are installed. In this mode, a compact version of the Desktop Bus (DBus) header is forwarded over the Catalyst bus, which provides the best possible centralized forwarding performance.

A fabric-enabled module has an additional connection directly to the switch fabric. Fabric-enabled modules forward packets in compressed mode, where only the header is sent to the Supervisor Engine and the full packet is forwarded directly from one line card to another.

To prevent use of nonfabric-enabled modules or to prevent fabric-enabled modules from using bus mode, enter the **nofabricswitching-modeallowbus-mode** command.

Caution Entering the **nofabricswitching-modeallowbus-mode** command removes power from any nonfabric-enabled modules that are installed.

The **fabricswitching-modeallow** c ommand affects Supervisor engines that are configured with a minimum of two fabric-enabled modules.

You can enter the **fabricswitching-modeallowtruncated** command to unconditionally allow truncated mode.

You can enter the **nofabricswitching-modeallowtruncated** command to allow truncated mode if the threshold is met.

You can enter the **nofabricswitching-modeallowbus-mode**command to prevent any module from running in bus mode.

To return to the default truncated-mode threshold, enter the **nofabricswitching-modeallowtruncatedthreshold** command.

The valid value for *mod*is the threshold value.

Examples

The following example shows how to specify truncated mode:

```
Router(config)#
fabric switching-mode allow truncated
```

Related Commands

Command	Description
ipv6 mfib hardware-switching uplink	Configures MFIB hardware switching for IPv6 multicast packets on a global basis.
show fabric	Displays the information about the crossbar fabric.

fabric switching-mode force bus-mode

To force fabric-enabled modules into bus switching mode, use the**fabricswitching-modeforcebus-mode** command in global configuration mode. To power cycle the module to truncated mode, use the **no** form of this command.

fabric switching-mode force bus-mode
no fabric switching-mode force bus-mode

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXD5	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 32.

This command applies to the following modules:

- WS-SVC-FWM-1-K9--Firewall Services Module
- WS-SVC-IDS2-BUN-K9--Intrusion Detection Service Module 2
- WS-SVC-MWAM-1--Multiprocessor WAN Application Module
- WS-SVC-NAM-1--Network Analysis Module 1
- WS-SVC-NAM-2--Network Analysis Module 2
- WS-SVC-PSD-1--Persistent Storage Device Module
- WS-SVC-SSL-1-K9--SSL Module
- WS-SVC-WLAN-1-K9--Wireless LAN Service Module

After you enter the **fabricswitching-modeforcebusmode** or the **nofabricswitching-modeforcebusmode**command, the fabric-enabled service modules power cycle immediately. The mode change occurs as the modules come up after the power cycle.

Examples

This example shows how to force fabric-enabled modules into flow-through switching mode:

```
Router(config)#
fabric switching-mode force bus-mode
Router(config)#
```

Related Commands

Command	Description
show fabric	Displays the information about the crossbar fabric.

fabric timer

To set the drop counter time-stamp and peak-utilization poll time in seconds, use the **fabrictimer**command in global configuration mode. To remove the drop counter time-stamp and peak-utilization poll time, use the **no** form of this command.

fabric timer *seconds*
no fabric timer *seconds*

Syntax Description

seconds	Poll time in seconds for drop counter time-stamps and peak-utilization. Valid values are from 1 to 1800.

Command Default

The internal default timer is set to 15 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SXF	This command was introduced on the Catalyst 6500 series switch.
12.2(5)SRB	This command was implemented on the Supervisor Engine 720.

Examples

The following example shows how to set the drop counter time-stamp and peak-utilization poll time to 200 seconds:

```
Router(config)#
fabric timer 200
```

Related Commands

Command	Description
show fabric	Displays the information about the crossbar fabric.

facility-alarm

To configure threshold temperatures for minor, major, and critical alarms, use the **facility-alarm** command in global configuration mode. To disable alarms for the threshold and reset the threshold to the default value, use the no form of this command.

Cisco 10000 Series Router

facility-alarm {**core-temperature** | **outlet-temperature**} {**major** | **minor** | **critical**} [*temperature*]

no facility-alarm {**core-temperature** | **outlet-temperature**} {**major** | **minor** | **critical**} [*temperature*]

Cisco 7200 Series Router

facility-alarm {**core-temperature** | **intake-temperature**} *temperature*

Syntax Description

core-temperature	Specifies that the alarm applies to the temperature of the internal core of the router. The temperature sensor close to the router's processor measures the core temperature.
outlet-temperature	Specifies that the alarm applies to the air flow temperature. **Note** This keyword is valid only on the Cisco 10000 series router for the PRE3.
major [*temperature*	Specifies the alarm threshold temperature threshold in degrees C. The default value is 53 degrees C. Major alarms affect several subscribers that connect to the reporting node.
minor [*temperature*	Specifies the alarm threshold temperature threshold in degrees C. The default value is 45 degrees C. Minor alarms affect a single or small number of subscribers who connect to the reporting node.
critical [*temperature*	Specifies the alarm threshold temperature threshold in degrees C. The default value is 85 Celsius C. Critical alarms affect most or all subscribers that connect to the reporting node.
temperature	Temperature threshold in degrees C. The range is 30 to 70 degrees C.

Command Default

If the command is not enabled, the default values are set.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(17)SL	This command was introduced on the Cisco 10000 series router.
12.2(16)BX	This command was introduced on the PRE2.
12.2(31)SB2	This command was introduced on the PRE3 for the Cisco 10000 series router.

Release	Modification
15.0(1)M	This command was integrated into a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelines

You can configure explicit threshold temperatures to override the defaults for major, minor, and critical alarms. Temperature thresholds for each alarm type and location are automatically set based on determined values that vary depending on the number and type of boards inserted in the chassis. In addition to the automatically set thresholds, you can set thresholds for minor and major temperature alarms. You can also disable the minor and major temperature alarms. You cannot, however, change the threshold for or disable critical alarms.

Cisco 10000 Series Router

On the PRE2, use the **facility-alarmcore-temperature** command. On the PRE3, use the **facility-alarmoutlet-temperature** command.

The default value for a threshold temperature depends on the performance routing engine (PRE) installed in the router as the following describes:

- Major alarm
  - PRE2--The default value is 53.
  - PRE3--The default value is 58.
- Minor alarm
  - PRE2--The default value is 45.
  - PRE3--The default value is 50.
- Critical alarm
  - PRE2--The default value is 85.
  - PRE3--The default value is 85.

Examples

The following example sets a threshold temperature of 53 for major alarms on the PRE2:

```
Router> enable
Router# config terminal
Router(config)# facility-alarm core-temperature major 53
```

The following example sets a threshold temperature of 50 for minor alarms on the PRE3:

```
Router> enable
Router# config terminal
Router(config)# facility-alarm core-temperature minor 50
```

Related Commands

Command	Description
clear facility-alarm	Clears alarm conditions and resets the alarm contacts.
show facility-alarm status	Displays the current major, minor, and critical alarm status, if any, and displays the configuration of the alarm thresholds.

facility-alarm critical exceed-action shutdown

To allow automatic router shutdown, use the facility-alarm critical exceed-action shutdown command in global configuration mode. To disable automatic router shutdown, use the **no** form of this command.

facility-alarm critical exceed-action shutdown
no facility-alarm critical exceed-action shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

Automatic router shutdown is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines

If the facility-alarm critical exceed-action shutdown command is enabled, the router performs an automatic shutdown under the following conditions:

- The internal temperature of the router or a power supply exceeds the temperature threshold.
- The voltage of an AC or DC power supply is out of tolerance.

Examples

The following example enables automatic router shutdown:

```
Router(config)# facility-alarm critical exceed-action shutdown
```

Related Commands

Command	Description
show facility-alarm	Displays the status of a generated alarm.

facility-alarm detect

To turn on the facility alarms, use the **facility-alarmdetect** command in global configuration mode. To turn off the alarm, use the **no** form of this command.

facility-alarm detect {**controller** *controller slot-number* | **interface** *type number* | **rps** | **temperature** | **fan**}
no facility-alarm detect {**controller T1** *slot-number* | **interface** *type number* | **rps** | **temperature** | **fan**}

Syntax Description

controller	Specifies the facility alarm for controllers.
controller slot-number	Specifies the controller. The controller can be one of the following: • **E1** --The range of the slot value is from 1 to 7 and the range of the port is from 0 to 7. • **T1** --The range of the slot value is from 1 to 7 and the range of the port is from 0 to 7. • **T3** --The range of the slot value is from 1 to 7.
interface	Specifies the facility alarm for interfaces.
type	Interface type. For more information, use the question mark (?) online help function.
number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
rps	Specifies the facility alarm for the redundant power supply (RPS).
temperature	Specifies the facility alarm for the environmental monitor temperature.
fan	Specifies the facility alarm for the environmental monitor fans.

Command Default

The facility alarm is turned off.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M on the Cisco 5400-XM series routers.

Usage Guidelines

Facility alarms monitor the following failure events:

- CT1/CE1/CT3 controller down
- Interface down
- RPS failure

- Trunk card failure

Cisco IOS software polls every second to detect the failure events that you have configured and turns on the alarm when any one of the failure events is detected. By default, the facility alarm is off. Users have to configure a facility alarm command to enable monitoring of the failure conditions.

Examples

The following example shows how to turn on the facility alarm for RPS:

```
Router(config)# facility-alarm detect rps
```

Related Commands

Command	Description
show facility-alarm	Displays the status of a generated alarm.

factory-reset all

To erase all the user-configured data, use the **factory-reset all** command in EXEC mode:

factory-reset all

Syntax Description

Syntax Description

This command has no keywords or arguments.

Command Modes

EXEC mode

Command History

Release	Modification
Cisco IOS XE Bengaluru Release 17.6.1	This command was introduced on ASR 900, ASR 920, and NCS 4200 platforms.

Usage Guidelines

The command erases the following data:

- All writable file systems and personal data
- OBFL logs
- User data and startup configuration
- ROMMON variables
- User credentials
- License information

Examples

The following example shows the configuration of the command:

```
Router>enable
Router>factory-reset all
```

factory-reset keep-licensing-info

To erase all the user-configured data except the licensing information, use the **factory-reset keep-licensing-info** command in EXEC mode:

factory-reset keep-licensing-info

Syntax Description

Syntax Description

This command has no keywords or arguments.

Command Modes

EXEC mode

Command History

Release	Modification
Cisco IOS XE Bengaluru Release 17.6.1	This command was introduced on ASR 900, ASR 920, and NCS 4200 platforms.

Usage Guidelines

This command erases the following user-configured data:

- All writable file systems and personal data
- OBFL logs
- User data and startup configuration
- ROMMON variables
- User credentials

Examples

The following example shows the configuration of the command:

```
enable
factory-reset keep-licensing-info
```

factory-reset all secure 3-pass

To erase all data using the the National Industrial Security Program Operating Manual (DoD 5220.22-M) Wiping Standard, use the **factory-reset all secure 3-pass-DoD 5220-22-M** command in EXEC mode:

factory-reset all-secure 3-pass-DoD 5220-22-M

Syntax Description

Syntax Description

This command has no keywords or arguments.

Command Modes

EXEC mode

Command History

Release	Modification
Cisco IOS XE Bengaluru Release 17.6.1	This command was introduced on ASR 900, ASR 920, and NCS 4200 platforms.

Usage Guidelines

The commands erases the following data

- All writable file systems and personal data using the the National Industrial Security Program Operating Manual (DoD 5220.22-M) Wiping Standard:
- OBFL logs
- User data and startup configuration
- ROMMON variables
- User credentials
- License information

Examples

The following example shows the configuration of the command:

```
enable
factory-reset all-secure 3-pass
DoD 5220-22-M
```

fddi burst-count

To allow the FCI card to preallocate buffers to handle bursty FDDI traffic (for example, Network File System [NFS] bursty traffic), use the **fddiburst-count** command in interface configuration mode. To revert to the default value, use the **no** form of this command.

fddi burst-count *number*
no fddi burst-count

Syntax Description

number	Number of preallocated buffers in the range from 1 to 10. The default is 3.

Command Default

3 buffers

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command applies to the FCI card only.

Note The microcode software version should *not* be 128.45 or 128.43.

Examples

The following example sets the number of buffers to 5:

```
Router(config)# interface fddi 0
Router(config-if)# fddi burst-count 5
```

fddi c-min

To set the C-Min timer on the pulse code modulation (PCM), use the **fddic-min** command in interface configuration mode. To revert to the default value, use the **no** form of this command.

fddi c-min *microseconds*
no fddi c-min

Syntax Description

microseconds	Sets the timer value, in microseconds. The default is 1600.

Command Default

1600 microseconds

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command applies to the processor connection management (CMT) only. You need extensive knowledge of the PCM state machine to tune this timer. Use this command when you run into PCM interoperability problems.

Examples

The following example sets the C-Min timer to 2000 microseconds:

```
Router(config)# interface fddi 0
Router(config-if)# fddi c-min 2000
```

Related Commands

Command	Description
fddi tb-min	Sets the TB-Min timer in the PCM.
fddi tl-min-time	Controls the TL-Min time (the minimum time to transmit a PHY line state before advancing to the PCM state, as defined by the X3T9.5 specification).
fddi t-out	Sets the t-out timer in the PCM.

fddi cmt-signal-bits

To control the information transmitted during the connection management (CMT) signaling phase, use the **fddicmt-signal-bits**command in interface configuration mode.

fddi cmt-signal-bits *signal-bits* [{**phy-a** | **phy-b**}]

Syntax Description

signal-bits	A hexadecimal number preceded by 0x; for example, 0x208. The FDDI standard defines 10 bits of signaling information that must be transmitted, as follows: • bit 0--Escape bit. Reserved for future assignment by the FDDI standards committee. • bits 1 and 2--Physical type, as defined in the first table below. • bit 3--Physical compatibility. Set if topology rules include the connection of a physical-to-physical type at the end of the connection. • bits 4 and 5--Link confidence test duration; set as defined in the second table below. • bit 6--MAC available for link confidence test. • bit 7--Link confidence test failed. The setting of bit 7 indicates that the link confidence was failed by the Cisco end of the connection. • bit 8--MAC for local loop. • bit 9--MAC on physical output.
phy-a	(Optional) Selects Physical Sublayer A. The default is 0x008 (hexadecimal) or 00 0000 1000 (binary). Bits 1 and 2 are set to 00 to select Physical A. Bit 3 is set to 1 to indicate “accept any connection.”
phy-b	(Optional) Selects Physical Sublayer B. The default is 0x20c (hexadecimal) or 10 0000 1100 (binary). Bits 1 and 2 are set to 10 to select Physical B. Bit 3 is set to 1 to indicate “accept any connection.” Bit 9 is set to 1 to select MAC on output. The normal data flow on FDDI is input on Physical A and output on Physical B.

Command Default

- **phy-a** is set to 0x008 (hexadecimal) or 00 0000 1000 (binary). Bits 1 and 2 are set to 00 to select Physical A. Bit 3 is set to 1 to indicate “accept any connection.”
- **phy-b** is set to 0x20c (hexadecimal) or 10 0000 1100 (binary). Bits 1 and 2 are set to 10 to select Physical B. Bit 3 is set to 1 to indicate “accept any connection.” Bit 9 is set to 1 to select MAC on output. The normal data flow on FDDI is input on Physical A and output on Physical B.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If neither the **phy-a** nor **phy-b** keyword is specified, the signal bits apply to both physical connections.

> **Caution** Use of the **fddicmt-signal-bits** configuration command is *not* recommended under normal operations. This command is used when debugging specific CMT implementation issues.

The table below lists the physical types.

Table 15: FDDI Physical Type Bit Specifications

Bit 2	Bit 1	Physical Type
0	0	Physical A
1	0	Physical B
0	1	Physical S
1	1	Physical M

The table below lists the duration bits.

Table 16: FDDI Link Confidence Test Duration Bit Specification

Bit 5	Bit 4	Test Duration
0	0	Short test (default 50 milliseconds)
1	0	Medium test (default 500 milliseconds)
0	1	Long test (default 5 seconds)
1	1	Extended test (default 50 seconds)

This command does not have a **no** form.

Examples

The following example sets the CMT signaling phase to signal bits 0x208 on both physical connections:

```
Router(config)# interface fddi 0
Router(config-if)# fddi cmt-signal-bits 0x208
```

fddi duplicate-address-check

To enable the duplicate address detection capability on the FDDI interface, use the **fddiduplicate-address-check** command in interface configuration mode. To disable this function, use the **no** form of this command.

fddi duplicate-address-check
no fddi duplicate-address-check

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If you use this command, the Cisco IOS software will detect a duplicate address if multiple stations are sharing the same MAC address. If the software finds a duplicate address, it will shut down the interface.

Examples

The following example enables duplicate address checking on the FDDI interface:

```
Router(config)# interface fddi 0
Router(config-if)# fddi duplicate-address-check
```

fddi encapsulate

To specify encapsulating bridge mode on the CSC-C2/FCIT interface card, use the **fddiencapsulate** command in interface configuration mode. To turn off encapsulation bridging and return the FCIT interface to its translational, nonencapsulating mode, use the **no**form of this command.

fddi encapsulate
no fddi encapsulate

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the FDDI interface uses the SNAP encapsulation format defined in RFC 1042, *Standard for the Transmission of IP Datagrams Over IEEE 802 Networks* . It is not necessary to define an encapsulation method for this interface when using the CSC-FCI interface card.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **nofddiencapsulate** command applies only to CSC-C2/FCIT interfaces, because the CSC-FCI interfaces are always in encapsulating bridge mode. The CSC-C2/FCIT interface card fully supports transparent and translational bridging for the following configurations:

- FDDI to FDDI
- FDDI to Ethernet
- FDDI to Token Ring

The **fddiencapsulate** command puts the CSC-C2/FCIT interface into encapsulation mode when doing bridging. In transparent mode, the FCIT interface interoperates with earlier versions of the CSC-FCI encapsulating interfaces when performing bridging functions on the same ring.

Caution Bridging between dissimilar media presents several problems that can prevent communications from occurring. These problems include bit-order translation (or usage of MAC addresses as data), maximum transfer unit (MTU) differences, frame status differences, and multicast address usage. Some or all of these problems might be present in a multimedia bridged LAN and might prevent communication from taking place. These problems are most prevalent when bridging between Token Rings and Ethernets or between Token Rings and FDDI nets. This is because of the different way Token Ring is implemented by the end nodes.

The following protocols have problems when bridged between Token Ring and other media: Novell IPX, DECnet Phase IV, AppleTalk, VINES, XNS, and IP. Furthermore, the following protocols may have problems when bridged between FDDI and other media: Novell IPX and XNS. We recommend that these protocols be routed whenever possible.

Examples

The following example sets FDDI interface 1 on the CSC-C2/FCIT interface card to encapsulating bridge mode:

```
Router(config)# interface fddi 1
Router(config-if)# fddi encapsulate
```

fddi frames-per-token

To specify the maximum number of frames that the FDDI interface transmits per token capture, use the **fddiframes-per-token** command in interface configuration mode. To revert to the default value, use the **no** form of this command.

fddi frames-per-token *number*
no fddi frames-per-token

Syntax Description

number	Maximum number of frames to transmit per token capture. Valid values are from 1 to 10. The default is 3.

Command Default

3 frames

Command Modes

Interface configuration

Command History

Release	Modification
11.2 P	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Changing the value will increase or decrease the maximum number of frames that the FDDI interface can transmit when it receives a token. Increasing the value does not necessarily mean more frames will be transmitted on each token capture. This is heavily dependent on the traffic load of the specific interface.

When the interface captures a token, it transmits all of the frames that are queued in the interface’s transmit ring, up to a maximum value specified by the**fddiframes-per-token** command.

If there are no frames ready for transmission, the token is passed on, and no frames are transmitted. If there are less than the **fddiframes-per-token**valuein the transmit ring, all frames in the transmit ring are transmitted before the token is passed on. If there are more than the **fddiframes-per-token**value in the transmit ring, the specified value is transmitted before the token is passed on. The remaining frames in the transmit ring remain queued until the token is captured again.

Examples

The following example shows how to configure the FDDI interface to transmit four frames per token capture:

```
Router(config-if)# fddi frames-per-token 4
```

fddi smt-frames

To enable the Station Management (SMT) frame processing capability on the FDDI, use the **fddismt-frames** command in interface configuration mode. To disable this function and prevent the Cisco IOS software from generating or responding to SMT frames, use the **no** form of this command.

fddi smt-frames
no fddi smt-frames

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **no** form of this command to turn off SMT frame processing for diagnosing purposes. Use the **fddismt-frames** command to reenable the feature.

Examples

The following example disables SMT frame processing:

```
Router(config)# interface fddi 0
Router(config-if)# no fddi smt-frames
```

fddi tb-min

To set the TB-Min timer in the physical connection management (PCM), use the **fdditb-min** command in interface configuration mode. To revert to the default value, use the **no** form of this command.

fddi tb-min *milliseconds*
no fddi tb-min

Syntax Description

milliseconds	Number, in milliseconds, that sets the TB-Min timer value. The range is from 0 to 65535. The default is 100.

Command Default

milliseconds : 100

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command applies to the processor connection management (CMT) only. Use this command when you run into PCM interoperability problems.

Note You need extensive knowledge of the PCM state machine to tune this timer.

Examples

The following example shows how to set the TB-Min timer to 200 ms:

```
Router(config)# interface fddi 0
Router(config-if)# fddi tb-min 200
```

Related Commands

Command	Description
fddi c-min	Sets the C-Min timer on the PCM.
fddi tl-min-time	Controls the TL-Min time (the minimum time to transmit a PHY line state before advancing to the PCM state, as defined by the X3T9.5 specification).
fddi t-out	Sets the t-out timer in the PCM.

fddi tl-min-time

To control the TL-Min time (the minimum time to transmit a Physical Sublayer, or PHY line state, before advancing to the next physical connection management [PCM] state, as defined by the X3T9.5 specification), use the **fdditl-min-time** command in interface configuration mode.

fddi tl-min-time *microseconds*

Syntax Description

microseconds	Number, in microseconds, that specifies the time used during the connection management (CMT) phase to ensure that signals are maintained for at least the value of TL-Min so that the remote station can acquire the signal. The range is from 0 to 4294967295. The default is 30.

Command Default

microseconds : 30

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Interoperability tests have shown that some implementations of the FDDI standard need more than 30 microseconds to sense a signal.

This command does not have a **no** form.

Examples

The following example changes the TL-Min time from 30 microseconds to 100 microseconds:

```
Router(config)# interface fddi 0
Router(config-if)# fddi tl-min-time 100
```

The following example changes the TL-Min time from 30 microseconds to 100 microseconds on a Cisco 7500 series router:

```
Router(config)# interface fddi 3/0
Router(config-if)# fddi tl-min-time 100
```

Related Commands

Command	Description
fddi c-min	Sets the C-Min timer on the PCM.
fddi t-out	Sets the t-out timer in the PCM.

fddi token-rotation-time

To control ring scheduling during normal operation and to detect and recover from serious ring error situations, use the **fdditoken-rotation-time** command in interface configuration mode. To revert to the default value, use the **no** form of this command.

fddi token-rotation-time *microseconds*
no fddi token-rotation-time

Syntax Description

microseconds	Number, in microseconds, that specifies the token rotation time (TRT). The range is from 4000 to 165000. The default is 5000.

Command Default

microseconds : 5000

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The FDDI standard restricts the allowed time to be greater than 4000 microseconds and less than 165,000 microseconds. As defined in the X3T9.5 specification, the value remaining in the TRT is loaded into the token holding timer (THT). Combining the values of these two timers provides the means to determine the amount of bandwidth available for subsequent transmissions.

Examples

The following example sets the rotation time to 24,000 microseconds:

```
Router(config)# interface fddi 0
Router(config-if)# fddi token-rotation-time 24000
```

The following example sets the rotation time to 24,000 microseconds on a Cisco 7500 series router:

```
Router(config)# interface fddi 3/0
Router(config-if)# fddi token-rotation-time 24000
```

fddi t-out

To set the timeout timer in the physical connection management (PCM), use the **fddit-out** command in interface configuration mode. To revert to the default value, use the **no** form of this command.

fddi t-out *milliseconds*
no fddi t-out

Syntax Description

milliseconds	Number, in milliseconds, that sets the timeout timer. The range is from 0 to 65535. The default is 100.

Command Default

milliseconds : 100

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command applies to the processor connection management (CMT) only. Use this command when you run into PCM interoperability problems.

Note You need extensive knowledge of the PCM state machine to tune this timer.

Examples

The following example sets the timeout timer to 200 ms:

```
Router(config)# interface fddi 0
Router(config-if)# fddi t-out 200
```

Related Commands

Command	Description
fddi c-min	Sets the C-Min timer on the PCM.
fddi tb-min	Sets the TB-Min timer in the PCM.
fddi tl-min-time	Controls the TL-Min time (the minimum time to transmit a PHY line state before advancing to the PCM state, as defined by the X3T9.5 specification).

fddi valid-transmission-time

To change the transmission valid timer (TVX) interval, use the**fddivalid-transmission-time** command in interface configuration mode. To revert to the default value, use the **no** form of this command.

fddi valid-transmission-time *microseconds* **fddi valid-transmission-time command**
no fddi valid-transmission-time

Syntax Description

microseconds	Number, in microseconds, that specifies the TVX interval. The range is from 2500 to 2147483647. The default is 2500.

Command Default

microseconds : 2500

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to recover from a transient FDDI ring error by setting a longer transmission timer interval.

Examples

The following example shows how to change the transmission timer interval to 3000 microseconds:

```
Router(config)# interface fddi 0
Router(config-if)# fddi valid-transmission-time 3000
```

The following example shows how to change the transmission timer interval to 3000 microseconds on Cisco 7000 series routers or Cisco 7200 series routers:

```
Router(config)# interface fddi 3/0
Router(config-if)# fddi valid-transmission-time 3000
```

fdl

To set the Facility Data Link (FDL) exchange standard for CSU controllers or to set the FDL exchange standard for a T1 interface that uses the Extended Super Frame (ESF) framing format, use the **fdl** command in interface configuration mode. To disable FDL support or to specify that there is no ESF FDL, use the **no** form of this command.

Cisco 2600 Series and Cisco 3600 Series Routers
fdl {**att** | **ansi** | **all** | **none**}
no fdl {**att** | **ansi** | **all** | **none**}

Cisco 10000 Series Router
fdl {**att** | **ansi**}
no fdl {**att** | **ansi**}

Syntax Description

att	Specifies AT&T technical reference 54016 for ESF FDL exchange support.
ansi	Specifies ANSI T1.403 for ESF FDL exchange support.
all	Specifies both AT&T technical reference 54016 and ANSI T1.403 for ESF FDL exchange support.
none	Specifies that there is no support for ESF FDL exchange.

Command Default

ANSI T1.403 for ESF FDL exchange support

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
12.0(5)XK	The **none** keyword was added, and the **both** keyword was changed to **all**.
12.0(5)T	The **none** keyword was added, and the **both** keyword was changed to **all**.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is available only for T1 links. This command sets the standard to be followed for FDL messaging through a 4-kbps out-of-band channel that a service provider uses to check for errors on the facility.

You must use the same FDL exchange standard as your service provider. If the setting is not correct, the link might not come up. You can configure a different standard on each T1 interface.

> **Note**
> When using a multiport T1 ATM IMA network module on a Cisco 2600 series or Cisco 3600 series router, ESF framing and binary eight zero substitution (B8ZS) line encoding are supported. When using a multiport E1 ATM IMA network module on a Cisco 2600 series or Cisco 3600 series router, CRC4 multiframe framing and HDB3 line encoding are supported. These are the parameters specified by the ATM Forum, and they cannot be changed.

Examples

Cisco 2600 and Cisco 3600 Series Routers

The following example shows how to specify the ANSI standard and the AT&T standard for FDL exchange:

```
Router(config)# interface atm 0/2
Router(config-if)# fdl all
```

Cisco 10000 Series Router

The following example shows how to specify the AT&T standard for FDL exchange:

```
Router(config)# interface atm 1/0/0
Router(config-if)# fdl att
```

flowcontrol

To configure a port to send or receive pause frames, use the **flowcontrol** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

flowcontrol {**send** | **receive**} {**desired** | **off** | **on**}
no flowcontrol {**send** | **receive**} {**desired** | **off** | **on**}

Syntax Description

send	Specifies that a port sends pause frames.
receive	Specifies that a port processes pause frames.
desired	Obtains predictable results regardless of whether a remote port is set to **on**, **off**, or **desired**.
off	Prevents a local port from receiving and processing pause frames from remote ports or from sending pause frames to remote ports.
on	Enables a local port to receive and process pause frames from remote ports or send pause frames to remote ports.

Command Default

Flow control is disabled.

Flow-control defaults depend upon port speed. The defaults are as follows:

- Gigabit Ethernet ports default to **off** for receive and **desired** for send.
- Fast Ethernet ports default to **off** for receive and **on** for send.
- On the 24-port 100BASE-FX and 48-port 10/100 BASE-TX RJ-45 modules, the default is **off** for receive and **off** for send.
- You cannot configure how WS-X6502-10GE 10-Gigabit Ethernet ports respond to pause frames. WS-X6502-10GE 10-Gigabit Ethernet ports are permanently configured to respond to pause frames.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	This command was implemented on the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.

Usage Guidelines

The **send** and **desired** keywords are supported on Gigabit Ethernet ports only.

Pause frames are special packets that signal a source to stop sending frames for a specific period of time because the buffers are full.

Gigabit Ethernet ports on the Catalyst 6500 series switches and on the Cisco 7600 series routers use flow control to inhibit the transmission of packets to the port for a period of time; other Ethernet ports use flow control to respond to flow-control requests.

If a Gigabit Ethernet port receive buffer becomes full, the port transmits a “pause” packet that tells remote ports to delay sending more packets for a specified period of time. All Ethernet ports (1000 Mbps, 100 Mbps, and 10 Mbps) can receive and act upon “pause” packets from other devices.

You can configure non-Gigabit Ethernet ports to ignore received pause frames (disable) or to react to them (enable).

When used with the **receive**keyword, the **on** and **desired** keywords have the same result.

All the Gigabit Ethernet ports on the Catalyst 6500 series switches and the Cisco 7600 series routers can receive and process pause frames from remote devices.

To obtain predictable results, follow these guidelines:

- Use **sendon** only when remote ports are set to **receiveon** or **receivedesired**.
- Use **sendoff** only when remote ports are set to **receiveoff** or **receivedesired**.
- Use **receiveon** only when remote ports are set to **sendon** or **senddesired**.
- Use **sendoff** only when remote ports are set to **receiveoff** or **receivedesired**.

Examples

These examples show how to configure the local port to not support any level of flow control by the remote port:

```
Router# configure terminal

Router(config)# interface GigabitEthernet1/9 10.4.9.157 255.255.255.0

Router(config-if)# flowcontrol receive off
Router(config-if)# flowcontrol send off
```

Related Commands

Command	Description
show interfaces flowcontrol	Displays flow-control information.

frame-relay

To configure Frame Relay payload compression for each Frame Relay port, use the **frame-relay**command in interface configuration mode. To terminate this form of payload compression over Frame Relay, use the **no** form of this command.

frame-relay payload-compression frf9 stac caim [*element-number*]
no frame-relay payload-compression

Syntax Description

payload-compression	Packet-by-packet payload compression, using the Stacker method.
frf9 stac	Enables FRF.9 compression using the Stacker method. If the router contains a data compression Advanced Interface Module (AIM) for the Cisco 2600 series router, compression is performed in the hardware (hardware compression). If the compression Advanced Interface Module (CAIM) is not available, compression is performed in the software installed on the main processor of the router (software compression).
caim *element-number*	Enable the data compression AIM hardware compression daughtercard to do compression, at the element numbered beginning with 0 and incrementing to include all possible elements.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.0(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **frame-relaypayload-compression** command to enable or disable payload compression on a point-to-point interface or subinterface. Use the **frame-relaymap** command to enable or disable payload compression on a multipoint interface or subinterface.

Shut down the interface before changing encapsulation types. Although this is not required, shutting down the interface ensures the interface is reset for the new encapsulation.

Examples

The following example shows Frame Relay configured to use payload compression with the frf9 stac algorithm for CAIM hardware compression, using the installed data compression AIM daughtercard as the compression source:

```
Router(config-if)# frame-relay payload-compression frf9 stac caim 0
```

Related Commands

Command	Description
compress stac caim	Specifies the exact hardware compression resource preferred.
encapsulation frame-relay	Enables Frame Relay encapsulation.
frame-relay interface-dlci	Assigns a DLCI to a specified Frame Relay subinterface on the router or access server.
frame-relay map	Defines mapping between a destination protocol address and the DLCI used to connect to the destination address.
show compress	Displays compression statistics.

framing

To select the frame type for the T1 or E1 data line, use the **framing** command in controller configuration mode.

T1 Lines
framing commandframing {**sfadm** | **esfadm**}

E1 Lines
framing {**crc4adm** | **pcm30adm** | **clear e1**}

Syntax Description

sfadm	Specifies super frame for the T1 channel.
esfadm	Specifies extended super frame for the T1 channel.
crc4adm	Specifies CRC4 framing mode for the E1 channel.
pcm30adm	Specifies CRC4 disabled framing mode for the E1 channel.
clear e1	Specifies clear-e1 framing mode for the E1 channel.

Command Default

Extended super frame (esf) for a T1 line CRC4 disabled framing (pcm30adm) for an E1 line

Command Modes

Controller configuration

Command History

Release	Modification
11.3	This command was introduced.
12.0(5)XE	The command was enhanced as an ATM interface configuration command.
12.0(7)XE1	This command was implemented on the Cisco 7100 series routers.
12.0(11)S	This command was integrated into Cisco IOS Release 12.0(11)S.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command in configurations in which the router or access server is intended to communicate with T1 or E1 fractional data lines. The service provided determines which framing type is required for your T1 or E1 circuit.

This command does not have a **no** form.

Examples

The following example selects extended super frame as the T1 frame type:

```
Router(config)# controller t1 4/0
Router(config-controller)# framing esfadm
```

Related Commands

Command	Description
lbo	Specifies the distance of the cable from the routers to the network equipment.
linecode	Selects the line code type for a T1 or E1 line.

framing (CEM)

To specify the framing format of a circuit emulation (CEM) T1 or E1 port, use the **framing** command in controller configuration mode. To reset the framing format of the port to its default value, use the **no** form of this command.

T1 Port
framing {**sf** | **esf** | **unframed**}
no framing

E1 Port
framing {**crc4** | **no-crc4** | **unframed**}
no framing

Syntax Description

sf	Specifies that the T1 port framing format is set to super frame (SF) format, also commonly known as D4 framing format.
esf	Specifies that the T1 port framing format is set to extended super frame (ESF) format. This is the default for a T1 line.
crc4	Specifies that the E1 port framing format is set to the G.704 standard with the optional CRC4 mechanism defined in time slot 0 enabled. This is the default for a E1 line. For Cisco NCS 4200 Series, crc4 is the default framing mode for E1 interface module.
no-crc4	Specifies that the E1 port framing format is set to the G.704 standard with the optional CRC4 mechanism defined in time slot 0 disabled.
unframed	Specifies that no framing structure is sought (on the ingress data stream) or imposed (on the egress data stream) on the T1 or E1 port. For Cisco NCS 4200 Series, unframed is the default framing mode for T1 interface module.

Command Default

The framing format of a T1 line defaults to **esf**. The framing format of an E1 line defaults to **crc4**. If an unframed CEM channel is created on the port using the **cem-group** command, no framing structure is sought or imposed.

Command Modes

Controller configuration

Command History

Release	Modification
12.3(7)T	This command was introduced to support circuit emulation.
XE 3.18SP	This command was integrated in the Cisco NCS 4200 Series.
XE Everest 16.5.1	This command was integrated in the Cisco NCS 4200 Series and Cisco ASR 903 Series Router.

Usage Guidelines

Framing must be configured to match the framing format used by the attached equipment.

In order to change a line between unframed and any framed mode, you must first delete the CEM channels defined in the line.

Examples

The following example shows how to set the framing format of a CEM T1 port to be super frame format.

```
Router(config-controller)# framing
 sf
```

The following example shows how to set the framing format of a CEM E1 port to the G.704 standard with the optional CRC4 mechanism defined in time slot 0 disabled.

```
Router(config-controller)# framing no-crc4
```

Examples

The following example shows how to set the framing format of a CEM T1 port for Cisco NCS 4200 Series.

```
Router(config-controller)# framingunframed
```

Examples

The following example shows how to set the framing format of a CEM E1 port for Cisco NCS 4200 Series and Cisco ASR 903 Series Router.

```
Router(config-controller)# framingcrc4
```

Related Commands

Command	Description
cem-group	Creates CEM channels on T1 or E1 ports.

framing (E3 controller)

To specify the type of framing used by the E3 controller, use the **framing**command in controller configuration mode. To restore the default framing type, use the **no** form of this command.

framing {**bypass** | **g751**}
no framing

Syntax Description

bypass	Specifies that G.751 framing be bypassed.
g751	Specifies G.751 as the E3 framing type. This is the default.

Command Default

G.751 framing

Command Modes

Controller configuration

Command History

Release	Modification
11.1 CA	This command was introduced.
12.2(11)YT	This command was integrated into Cisco IOS Release 12.2(11)YT and implemented on the following platforms for E3: Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3660 series, Cisco 3725, and Cisco 3745 routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If you do not specify the framing command, the default, **g751**, is used by the E3 controller to automatically determine the framing type received from the far-end equipment.

Configure framing as G.751 when the E3 connection terminates remotely on a Digital Link or Kentrox data service unit (DSU), or when needing a subrate on an E3 connection between two T3 or E3 network modules.

Note The local interface configuration must match the remote interface, or DSU, configuration.

When G.751 framing is used, DSU bandwidth can be used to select a payload subrate from 34,010 kbps down to 22 kbps.

When framing bypass is used, DSU bandwidth of 34,010 kbps must be configured.

When G.751 framing is used, configuring the scramble command can prevent some payload data from being mistakenly interpreted as G.751 framing bits by switches placed between the DSUs. By default, the no scramble command is configured.

When framing bypass is used, the no scramble command must be configured.

When G.751 framing is used, bit 11 of the G.751 frame is reserved for national use and is set to 1 by default. Configure national bit 1 only when required for interoperability with your telephone company.

Examples

The following example shows the framing for the E3 controller set to bypass:

```
Router(config)# controller e3 1/0
Router(config-controller)# framing bypass
```

Related Commands

Command	Description
scramble	Specifies the type of framing used by the T1 channels on the CT3IP in Cisco 7500 series routers.

framing (SONET)

To select the frame type of the frame received on an optical line, use the **framing**command in controller configuration mode.

framing {**sonet** | **sdh**}

Syntax Description

sonet	Specifies the framing type as SONET.
sdh	Specifies the framing type as Synchronous Digital Hierarchy (SDH).

Command Default

SONET is the default for the PA-MC-STM-1 port adapter. SDH is the default for the STM-1 trunk card.

Command Modes

Controller configuration

Command History

Release	Modification
12.0(14)S	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T and support was added for the STM-1 trunk card on the Cisco AS5850 platform.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
XE Everest 16.5.1	This command was introduced on the Cisco ASR 920 Routers and Cisco NCS 4200 Series.

Usage Guidelines

Use this command to configure the framing type of the SONET controller. The PA-MC-STM-1 port adapter supports both the SONET and SDH framing modes. The STM-1 trunk feature card on the Cisco AS5850 supports only SDH framing.

This command does not have a **no** form.

Examples

The following example shows how to configure the framing type on a SONET controller of an STM-1 card in physical slot number 2 on a Cisco AS5850:

```
Router(config)# controller sonet 2/0
Router(config-controller)# framing sonet
```

Related Commands

Command	Description
show controllers sonet	Displays information about SONET controllers.

framing (T1 E1 controller)

To select the frame type for the T1 or E1 data line, use the **framing** command in controller configuration mode. To return to the default, use the **no** form of the command.

T1 Lines
framing {**sf** | **esf**}

E1 Lines
framing {**crc4** | **no-crc4**} [**australia**]

T1 Shared Port Adapter
framing {**sf** | **esf**}
no framing {**sf** | **esf**}

E1 Shared Port Adapter
framing {**crc4** | **no-crc4** | **unframed**}
no framing {**crc4** | **no-crc4** | **unframed**}

Syntax Description

sf	Specifies super frame as the T1 frame type. This is the default.
esf	Specifies extended super frame as the T1 frame type.
crc4	Specifies CRC4 as the E1 frame type. This is the default for Australia.
no-crc4	Specifies CRC4 disabled as the E1 frame type.
unframed	Specifies unframed mode.
australia	(Optional) Specifies the E1 frame type used in Australia.

Command Default

sf on a T1 line

crc4 on an E1 line

Command Modes

Controller configuration

Command History

12.2S	This command was integrated into Cisco IOS Release 12.2S.
12.2(25)S3	This command was integrated into Cisco IOS Release 12.2(25)S3.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE to support SPAs on a Cisco 7600 series router and Catalyst 6500 series switch.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.1(2)SNH	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Use this command in configurations in which the router or access server is intended to communicate with T1 or E1 fractional data lines. The service provider determines the framing type required for your T1/E1 circuit.

To return to the default mode on a T1/E1 SPA, use the **no** form of this command. This command does not have a **no** form for other T1/E1 lines.

Examples

The following example selects extended super frame as the T1 frame type:

```
Router(config-controller)# framing esf
```

Related Commands

Command	Description
cablelength	Specifies the distance of the cable from the routers to the network equipment.
linecode	Selects the linecode type for T1 or E1 line.

framing (T3 controller)

To choose framing mode on a T3 port, use the **framing**command in controller configuration mode. To return to the default mode, use the no form of this command.

T3 Controllers
framing {**c-bit** | **m23**}
no framing

Channelized T3 Shared Port Adapters and the Cisco 7500 Series Routers with CT3IP Port Adapter
framing {**c-bit** | **m23** | **auto-detect**}
no framing

Syntax Description

auto-detect	Specifies detection of the framing type that it receives from the far-end equipment.
c-bit	Specifies that C-bit framing is used as the T3 framing type.
m23	Specifies that M23 framing is used as the T3 framing type.

Command Default

c-bit (for the 2-Port and 4-Port Channelized T3 SPA and most T3 controllers)

auto-detect (for the CT3IP in a Cisco 7500 series router)

Command Modes

Controller configuration

Command History

Release	Modification
11.1CA	This command was introduced.
12.2(11)YT	This command was integrated into Cisco IOS Release 12.2(11)YT and implemented on the following platforms for T3: Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3660 series, Cisco 3725, and Cisco 3745 routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2S	This command was integrated into Cisco IOS Release 12.2S.
12.2(25)S3	This command was integrated into Cisco IOS Release 12.2(25)S3 to support SPAs on the Cisco 7304 routers.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE to support SPAs on a Cisco 7600 series router or Catalyst 6500 series switch.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S to support SPAs on the Cisco 12000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You can set the framing for each T1 channel by using the **t1framing**controller configuration command.

Cisco 7500 Series Routers with CT3IP Port Adapter

Because the CT3IP supports the Application Identification Channel (AIC) signal, the setting for the framing might be overridden by the CT3IP firmware.

Examples

The following example sets the framing mode on a T3 interface.

```
Router# configure terminal
Router(config)# controller t1 6/0/0
Router(config-controller)# framing m23
```

The following example sets the framing for the CT3IP to C-bit:

```
Router(config)# controller t3 9/0/0
Router(config-controller)# framing c-bit
```

Related Commands

Command	Description
controller	Configures a T1, E1, or T3 controller and enters controller configuration mode.
show controller	Displays controller configuration.
t1 framing	Specifies the type of framing used by the T1 channels.

framing (T3-E3 interface)

To choose framing mode on a T3 or E3 port, use the **framing**command in interface configuration mode. To return to the default mode, use the no form of this command.

PA-T3 and T3 Shared Port Adapters
framing {**bypass** | **c-bit** | **m13**}
no framing {**bypass** | **c-bit** | **m13**}

PA-E3 and E3 Shared Port Adapters
framing {**bypass** | **g751** | **g832**}
no framing {**bypass** | **g751** | **g832**}

Syntax Description

bypass	Bypasses DS3 framing mode.
c-bit	Enables DS3 C-bit framing mode.
m13	Enables DS3 M13 framing mode.
g751	Enables E3 G.751 framing mode.
g832	Enables E3 G.832 framing mode. The g832 keyword is not supported on Cisco 7304 routers with the 4-Port Clear Channel T3/E3 SPA.

Command Default

T3: C-bit framing

E3: g751 framing

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2S	This command was integrated into Cisco IOS Release 12.2S.
12.2(25)S3	This command was integrated into Cisco IOS Release 12.2(25)S3 to support SPAs on the Cisco 7304 routers.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE to support SPAs on a Cisco 7600 series router and Catalyst 6500 series switch. The **g832** keyword option was added to the command.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S to support SPAs on the Cisco 12000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The default framing is described in the ITU-T Recommendation G.751.

Note The International Telecommunication Union Telecommunication Standardization Sector (ITU-T) carries out the functions of the former Consultative Committee for International Telegraph and Telephone (CCITT).

When the framing mode is **bypass**, the T3 frame data is not included in the T3 frame, just the data.

When the framing mode is **bypass**, the E3 frame data is not included in the E3 frame, just the data.

If you use the **bypass** keyword, scrambling must be set to the default (disabled), the DSU mode must be set to the default (0), and the DSU bandwidth must be set to the default (44736).

The g832 keyword is not supported on Cisco 7304 routers with the 2-Port and 4-Port Clear Channel T3/E3 SPA.

Examples

The following example sets the framing mode to bypass on interface 1/0/0:

```
Router(config)# interface serial 1/0/0
Router(config-if)# framing bypass
```

Related Commands

Command	Description
show controller serial	Displays serial line statistics.

full-duplex

To specify full-duplex mode on full-duplex single-mode and multimode port adapters, use the **full-duplex**command in interface configuration mode. To restore the default half-duplex mode, use the **no** form of this command.

full-duplex
no full-duplex

Syntax Description

This command has no arguments or keywords.

Command Default

Half-duplex; a Fast Ethernet Interface Processor (FEIP), and serial interfaces that are configured for bisynchronous tunneling

Autonegotiation

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
11.3	This command was modified to include information on FDDI full-duplex, single-mode, and multimode port adapters.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command if the equipment on the other end is capable of full-duplex mode.

This command specifies full-duplex mode on full-duplex single-mode and multimode port adapters available on the following networking devices:

- Cisco 7200 series routers
- Second-generation Versatile Interface Processors (VIP2s) in Cisco 7500 series routers
- FEIP ports
- Serial interface ports that uses bisynchronous tunneling

Refer to the *CiscoProductCatalog* for hardware compatibility information and for specific model numbers of port adapters.

To enable half-duplex mode, use the **nofull-duplex** or **half-duplex** command.

Note For the Cisco AS5300, the **duplexfull**| **halfauto**} command replaces the **full-duplex** and **half-duplex** commands. You will get the following error messages if you try to use the **full-duplex** and **half-duplex** commands on a Cisco AS5300: Router(config)# **interfacefastethernet0** Router(config-if)# **full-duplex** Please use duplex command to configure duplex mode Router(config-if)# Router(config-if)# **half-duplex** Please use duplex command to configure duplex mode

Support for This Command

Use the question mark (?) command to find out which port adapters support this command. If the interface does not support full-duplex, an informational message displayed, and no changes are made to the interface. To determine if the interface supports full-duplex, use the **showinterfaces**command. For example, the following message is displayed if the interface does not support full-duplex:

```
% interface does not support full-duplex.
```

Use on FDDI

Full-duplex on the FDDI full-duplex port adapters allows an FDDI ring with exactly two stations to transform the ring into a full-duplex, point-to-point topology. For the interface to operate in full-duplex mode, there must be only two stations on the ring, the two stations must be capable of operating in full-duplex mode, and both stations must complete a full-duplex autoconfiguration protocol. There is no FDDI token in full-duplex mode. Refer to the *CiscoProductCatalog* for specific model numbers of port adapters.

Full-duplex autoconfiguration protocol allows an FDDI station to dynamically and automatically operate in either half-duplex (or ring) or full-duplex mode, and ensures that the stations fall back to ring mode when a configuration change occurs, such as a third station joining the ring.

After booting the router, the FDDI stations begin operation in half-duplex mode. While the station performs the full-duplex autoconfiguration protocol, the station continues to provide data-link services to its users. Under normal conditions, the transition between half-duplex mode and full-duplex mode is transparent to the data-link users. The data-link services provided by full-duplex mode are functionally the same as the services provided by half-duplex mode.

If you change the full-duplex configuration (for example, from disabled to enabled) on supported interfaces, the interface resets.

Cisco 10000 Series Router

The Fast Ethernet line card responds only to 802.3x pause frames from another device when it autonegotiates the duplex mode (the default). The line card does not support 802.3x flow control when you manually set half-duplex or full-duplex mode.

Examples

Cisco 7200 Series Router

The following example configures full-duplex mode on the Cisco 7200 series routers:

```
Router(config)# interface fastethernet 0/1
Router(config-if)# full-duplex
```

Full-Duplex Binary Synchronous

The following example specifies full-duplex binary synchronous communications (Bisync) mode:

```
Router(config)# interface serial 0
Router(config-if)# encapsulation bstun
Router(config-if)# full-duplex
```

Full-Duplex on FDDI Interface

The following example enables full-duplex mode on FDDI interface 0:

```
Router(config)# interface fddi 0/1/0
Router(config-if)# full-duplex
```

Related Commands

Command	Description
half-duplex	Specifies half-duplex mode on an SDLC interface or on the FDDI full-duplex, single-mode port adapter and FDDI full-duplex, multimode port adapter on the Cisco 7200 series and Cisco 7500 series routers.
interface	Configures an interface type and enters interface configuration mode.
interface fastethernet	Selects a particular Fast Ethernet interface for configuration.
interface serial	Specifies a serial interface created on a channelized E1 or channelized T1 controller (for ISDN PRI, CAS, or robbed-bit signaling).
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show interfaces fddi	Displays information about the FDDI interface.

g709 disable

To disable the ITU-T G.709 wrapper, use the **g709 disable** command in DWDM configuration mode. To enable the ITU-T G.709 wrapper, use the **no** form of this command.

g709 disable

no g709 disable

Syntax Description

Syntax Description

This command has no keywords or arguments.

Command Default

The G.709 wrapper is enabled.

Command Modes

DWDM configuration

Command History

Release	Modification
XE 3.18SP	Support for this command was introduced on NCS 4200 Series router.

Usage Guidelines

To display the G.709 alarms and counters, use the**show controller dwdm g709** command.

Examples

The G.709 wrapper is enabled by default. The following example shows how to disable the G.709 wrapper on an interface:

```
enable
configure terminal
controller dwdm 0/0/0
g709 disable
end
```

If you have disabled the G.709 wrapper using the **g709 disable** command, use the **no g709 disable** command to re-enable it, as shown in the following example:

```
enable
configure terminal
controller dwdm 0/0/0
no g709 disable
end
```

Related Commands

Command	Description
show controller dwdm	Displays DWDM controller configuration.

g709 fec

To configure the forward error correction (FEC) mode for the DWDM controller, use the **g709fec**command in controller configuration mode. To return to the default state, use the **no** form of this command.

g709 fec {**disable** | **enhanced** | **standard**}
no g709 fec

Syntax Description

disable	Disables FEC.
enhanced	Enables enhanced FEC mode.
standard	Enables standard FEC mode.

Command Default

Standard FEC mode is enabled by default.

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
12.2(33)SRD1	This command was introduced on the Cisco 7600 series router.

Usage Guidelines

The **g709fec** command can be used only when the DWDM controller is in the shutdown state.

Standard FEC is the default mode; therefore, if you use the **nog709fec** command, standard FEC is used.

Examples

The following example shows how to configure standard FEC mode on a DWDM controller:

```
Router(config)# controller dwdm 1/3
Router(config-controller)# g709 fec standard
```

Related Commands

Command	Description
controller dwdm	Configures a DWDM controller.
g709 odu threshold	Configures thresholds for selected ODU BER alarms.
g709 otu threshold	Configures thresholds for selected OTU BER alarms.
no g709 odu report	Disables the logging of selected ODU alarms.
no g709 otu report	Disables the logging of selected OTU alarms.
show controller dwdm	Displays ITU-T G.709 alarms, alerts, and counters.
transport-mode	Configures a transport mode.

g709 odu report

To enable the logging of selected optical channel data unit (ODU) alarms to the console for a DWDM controller, use the **g709odureport**command in controller configuration mode. To disable logging, use the no form of this command.

g709 odu report {**ais** | **bdi** | **lck** | **oci** | **pm-tca** | **ptim** | **sd-ber** | **sf-ber** | **tim**}
no g709 odu report {**ais** | **bdi** | **lck** | **oci** | **pm-tca** | **ptim** | **sd-ber** | **sf-ber** | **tim**}

Syntax Description

ais	Alarm indication signal reporting status.
bdi	Backward defect indication reporting status.
lck	Upstream connection locked reporting status.
oci	Open connection indication error reporting status.
pm-tca	Path monitoring BER TCA reporting status.
ptim	Payload type identifier mismatch reporting status.
sd-ber	Sets PM BER in excess of SD threshold reporting status.
sf-ber	Sets PM BER in excess of SF threshold reporting status.
tim	Sets Trace Identifier Mismatch reporting status.

Command Default

Logging is enabled for all keywords.

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
12.2(33)SRD1	This command was introduced on the Cisco 7600 series router.

Usage Guidelines

This command can be used only when the DWDM conroller is in the shutdown state.

Examples

The following example shows how to enable ODU reporting for OCI:

```
Router(config)# controller dwdm 1/2
Router(config-controller)# g709 odu report oci
```

Related Commands

Command	Description
controller dwdm	Configures a DWDM controller.
g709 fec	Configures the FEC for the DWDM controller.
g709 odu threshold	Configures thresholds for selected ODU BER alarms.

Command	Description
g709 otu threshold	Configures thresholds for selected OTU BER alarms.
show controller dwdm	Displays G.709 alarms, alerts, and counters.
show platform dwdm alarm history	Displays platform DWDM alarm history.

g709 odu overhead tti

To configure the Trail Trace Identifier (TTI) level for an Optical Channel Data Unit (ODU), use the **g709oduoverheadtti**command in DWDM configuration mode. To return to the default, use the **no** form of this command.

g709 odu overhead tti {**expected** | **sent**} {**ascii** | **hex**} *tti-string*
no g709 odu overhead tti {**expected** | **sent**} {**ascii** | **hex**} *tti-string*

Syntax Description

expected	Configures the expected TTI string.
sent	Configures the transmit TTI string.
ascii	Indicates that the string is in ASCII format.
hex	Indicates that the string is in hexidecimal format.
tti-string	The TTI level string. You can configure the TTI level string in ASCII string format or hexadecimal format. The ASCII text string can be a maximum of 64 characters. The hexadecimal string length must be an even number and can be a maximum of 128 bytes.

Command Default

No TTI level string is configured.

Command Modes

DWDM configuration.

Command History

Release	Modification
15.1(2)S	This command was introduced on the Cisco 7600 Router.

Usage Guidelines

To display the TTI strings, use the **showcontrollerdwdmg709** command.

Examples

The following example shows how to configure the expected TTI string:

```
Router(config)# controller dwdm 0/1/0/0
Router(config-dwdm)# g709 odu overhead tti expected ascii test_odu_5678
```

Related Commands

Command	Description
show controller dwdm	Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.

g709 odu threshold

To configure thresholds for selected optical channel data unit (ODU) bit error rate (BER) alarms, use the **g709oduthreshold**command in controller configuration mode. To return to the default state, use the **no** form of this command.

g709 odu threshold {**pm-tca** **bit-error-rate** | **sd-ber** **bit-error-rate** | **sf-ber** **bit-error-rate**}
no g709 odu threshold {**pm-tca** **bit-error-rate** | **sd-ber** **bit-error-rate** | **sf-ber** **bit-error-rate**}

Syntax Description

pm-tca	Sets the path monitoring threshold crossing alert threshold.
sd-ber	Sets the signal degrade bit error rate (BER) threshold.
sf-ber	Sets the signal failure BER threshold.
bit-error-rate	Specifies the BER threshold value in the range from 3 through 9. The threshold value is interpreted as a negative exponent of 10 when determining the bit error rate. For example, a value of 5 implies a bit error rate of 10 to the minus 5. The default BER threshold value is 6.

Command Default

sd-ber: 6

sf-ber: 3

pm-tca: 3

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
12.2(33)SRD1	This command was introduced on the Cisco 7600 series router.

Usage Guidelines

This command can be used only when the DWDM controller is in the shutdown state.

Examples

The following example shows how to set the signal fail BER rate to 5:

```
Router(config)# controller dwdm 1/2
Router(config-controller)# g709 odu threshold sf-ber 5
```

Related Commands

Command	Description
controller dwdm	Configures a DWDM controller.
g709 fec	Configures the FEC for the DWDM controller
g709 otu threshold	Configures thresholds for selected OTU BER alarms.
no g709 odu report	Disables the logging of selected ODU alarms.
no g709 otu report	Disables the logging of selected OTU alarms.

Command	Description
show controller dwdm	Displays ITU-T G.709 alarms, alerts, and counters.
transport-mode	Configures a transport mode.

g709 otu report

To enable the logging of selected optical channel transport unit (OTU) alarms to the console for a DWDM controller, use the **g709otureport**command in controller configuration mode. To disable logging, use the no form of this command.

g709 otu report {**ais** | **bdi** | **iae** | **lof** | **lom** | **los** | **sm-tca** | **tim** | **sd-ber** | **sf-ber**}
no g709 otu report {**ais** | **bdi** | **iae** | **lof** | **lom** | **los** | **sm-tca** | **tim** | **sd-ber** | **sf-ber**}

Syntax Description

ais	Alarm indication signal reporting status.
bdi	Backward defect indication reporting status.
iae	Incoming alignment error reporting status.
lof	OTU loss of frame reporting status.
lom	Loss of multiple frame reporting status.
los	Loss of signal reporting status.
sm-tca	Section monitoring BER TCA reporting status.
tim	Trace identifier mismatch reporting status.
sd-ber	SM BER is in excess of the SD BER threshold
sf-ber	SM BER is in excess of the SF BER threshold

Command Default

Reporting is enabled for all keywords.

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
12.2(33)SRD1	This command was introduced on the Cisco 7600 series router.
XE 3.18SP	This command was introduced on the Cisco NCS 4200 Series router.

Usage Guidelines

This command can be used only when the DWDM controller is in the shutdown state.

Examples

The following example shows how to enable OTU reporting for IAE:

```
Router(config)# controller dwdm 1/2
Router(config-controller)# g709 otu report iae
```

Related Commands

Command	Description
controller dwdm	Configures a DWDM controller.

Command	Description
g709 fec	Configures the FEC for the DWDM controller.
g709 odu threshold	Configures thresholds for selected ODU BER alarms.
g709 otu threshold	Configures thresholds for selected OTU BER alarms.
no g709 odu report	Disables the logging of selected ODU alarms.
show controller dwdm	Displays ITU-T G.709 alarms, alerts, and counters.
show platform dwdm alarm history	Displays platform DWDM alarm history.
transport-mode	Configures a transport mode.

g709 otu threshold

To configure thresholds for selected optical channel transport unit (OTU) bit error rate (BER) alarms, use the **g709otuthreshold**command in controller configuration mode. To return to the default state, use the **no** form of this command.

g709 otu threshold sm-tca| sd-ber| sf-ber bit-error-rate
no g709 otu threshold sm-tca| sd-ber| sf-ber bit-error-rate

Syntax Description

sm-tca	Sets the Section Monitoring Threshold Crossing Alert threshold.
sd-ber	Sets the Signal Degrade Bit Error rate threshold.
sf-ber	Sets the Signal Failure Bit Error Rate threshold.
bit-error-rate	Sets the BER threshold value in the range from 3 through 9. The threshold value is interpreted as a negative exponent of 10 when determining the bit error rate. For example, a value of 5 implies a bit error rate of 10 to the minus 5. The default BER threshold value is 3.

Command Default

bit-error-rate: 3

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
12.2(33)SRD1	This command was introduced on the Cisco 7600 series router.
XE 3.18 SP	This command was introduced on the Cisco NCS 4200 Series router.

Usage Guidelines

This command can be used only when the DWDM controller is in the shutdown state.

Examples

The following example shows how to set the Section Monitoring Threshold Crossing Alert threshold to 5:

```
Router(config)# controller dwdm 1/2
Router(config-controller)# g709 otu threshold sm-tca 5
```

Related Commands

Command	Description
controller dwdm	Configures a DWDM controller.
g709 fec	Configures the FEC for the DWDM controller.
g709 odu threshold	Configures thresholds for selected ODU BER alarms.
no g709 odu report	Disables the logging of selected ODU alarms.
no g709 otu report	Disables the logging of selected OTU alarms.

Command	Description
show controller dwdm	Displays ITU-T G.709 alarms, alerts, and counters.
transport-mode	Configures a transport mode.

g709 tti-processing enable

To configure Trail Trace Identifier (TTI), use the **g709 tti-processing enable** command in the controller configuration mode.

g709 tti-processing enable {*odu* | *otu*}

Syntax Description

Syntax Description

odu	Configures TTI for selected ODU alarm.
otu	Configures TTI for selected OTU alarm.

Command Modes

Controller configuration

Command History

Release	Modification
15.6(02)SP	Support for this command was introduced on NCS 4200 Series router.

Usage Guidelines

The interface goes down in case of OTU TIM or ODU TIM alarms.

Examples

The following example shows how to enter CEM interface parameters:

```
enable
configure terminal
controller dwdm 0/4/1
shutdown
g709 tti-processing enable odu
no shutdown
end
```

Related Commands

Command	Description
clear controller dwdm	Displays the DWDM controller configuration.

gnss

To enable the global navigation satellite system (GNSS) module on the Cisco ASR 903, Cisco ASR 907, and the Cisco ASR 920 routers, use the **gnss** command in the global configuration mode.

gnss slot {*r0r1*}

Syntax Description

slot	Specifies the slot information.
r0	Indicates route processor slot 0.
r1	Indicates route processor slot 1.

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
IOS-XE 3.17	This command was introduced on the Cisco ASR 903, Cisco ASR 907, and the Cisco ASR 920 routers.

Usage Guidelines

This command enables the GNSS module on the router. However, you must execute the **no shutdown** command after the **gnss** command to ensure that the interface is administratively up.

Examples

The following example shows how to enable the GNSS module and enter the GNSS mode:

```
Router# configure terminal
Router(config)# gnss slot r0
Router(config-gnss)# no shutdown
```

Related Commands

Command	Description
1pps	Configures the pulse per second from the GNSS module.
anti-jam	Enables or disables the anti-jam mode on the GNSS module.
constellation	Configures the GNSS module based on the specified satellite constellations.
default	Resets the device to its default state.
exit	Exists the GNSS sub mode.
no	Negates the command or sets the value of the command to its default values.
shutdown	Enables GNSS module.

gtp

To enables Enhanced Wireless Access Gateway (EWAG) General packet radio service (GPRS) Tunneling Protocol (GTP) and enter EWAG GTP configuration mode, use the **gtp** command in global configuration mode.

gtp

Syntax Description

This command does not contain any keywords or arguments.

Command Default

This command has no defaults.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Examples

The following example shows how to enable GTP and configure parameters of an access point.

```
Device(config)# gtp
Device(config-gtp)# n3-request 3
Device(config-gtp)# interval t3-response 30
Device(config-gtp)# information-element rat-type wlan
Device(config-gtp)# interface local GigabitEthernet0/0/0
WARNING: same interface has already been configured
Device(config-gtp)# apn 1
Device(config-gtp-apn)#  apn-name starent.com
Device(config-gtp-apn)#  ip address ggsn 10.1.2.1
Device(config-gtp-apn)#  dns-server 10.1.2.1
Device(config-gtp-apn)#  dhcp-server 10.10.197.1
Device(config-gtp-apn)#  dhcp-lease 6000
Device(config-gtp-apn)#  tunnel mtu 1500
Device(config-gtp-apn)# end
```

Related Commands

Command	Description
apn	Configures an ASCII regular expression string to be matched against the APN for GPRS load balancing.
apn-name	Configures access point name.
debug gtp	Debugs information related to EWAG GTP.

Command	Description
dns-server	Specifies the DNS IP servers available to a DHCP client.
dhcp-server	Specifies a primary (and backup) DHCP server to allocate IP addresses to MS users entering a particular PDN access point.
dhcp-lease	Configures DHCP lease time in seconds.
interval (EWAG)	Configures message intervals.
information-element	Configures information elements.
interface (EWAG)	Configure EWAG interface.
ip address ggsn	Configures GGSN IP address.
n3-request	Specifies the maximum number of times that the quota server attempts to send a signaling request to the CSG.
show gtp	Displays information related to EWAG GTP.
tunnel mtu	Configures GTP tunnel parameters.

half-duplex

To specify half-duplex mode on an Synchronous Data Link Control (SDLC) interface or on the FDDI full-duplex, single-mode port adapter and FDDI full-duplex, multimode port adapter on the Cisco 7200 series and Cisco 7500 series routers, use the **half-duplex** command in interface configuration mode. To reset the interface to full-duplex mode, use the **no** form of this command.

half-duplex
no half-duplex

Syntax Description

This command has no arguments or keywords.

Command Default

Full-duplex mode is the default mode on an SDLC interface, the FDDI full-duplex, single-mode port adapter and FDDI full-duplex, multimode port adapter on the Cisco 7200 series and Cisco 7500 series routers.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
11.3	This command was modified to include information on FDDI full-duplex, single-mode, and multimode port adapters.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

SDLC Interfaces

The **half-duplex** command is used to configure an SDLC interface for half-duplex mode and is used on a variety of port adapters. Use the question mark (?) command to find out which port adapters support this command.

Note The **half-duplex**command replaces the **sdlchdx** and **media-typehalf-duplex** commands.

Note For the Cisco AS5300, the **duplexfullhalfauto**} command replaces the **full-duplex** and **half-duplex** commands. You will get the following error messages if you try to use the **full-duplex** and **half-duplex** commands on a Cisco AS5300: Router(config)# **interfacefastethernet0** Router(config-if)# **full-duplex** Please use duplex command to configure duplex mode Router(config-if)# Router(config-if)# **half-duplex** Please use duplex command to configure duplex mode

Enabling Full-Duplex Mode

To enable full-duplex mode, use the **nohalf-duplex**or**full-duplex**commands.

Note The **media-typehalf-duplex** command exists in Cisco IOS Release 11.0(5). As of Release 11.0(6), the keyword **half-duplex** was removed from the **media-type** command. In Release 11.0(6), the functionality for specifying half-duplex mode is provided by the**half-duplex** command.

Port Adapters

Refer to the *CiscoProductCatalog* for specific model numbers of port adapters.

Examples

The following example configures an SDLC interface for half-duplex mode:

```
Router(config-if)# encapsulation sdlc-primary
Router(config-if)# half-duplex
```

Related Commands

Command	Description
full-duplex	Specifies full-duplex mode on full-duplex single-mode and multimode port adapters.

half-duplex controlled-carrier

To place a low-speed serial interface in controlled-carrier mode, instead of constant-carrier mode, use the **half-duplexcontrolled-carrier**command in interface configuration mode. To return the interface to constant-carrier mode, use the **no** form of this command.

half-duplex controlled-carrier
no half-duplex controlled-carrier

Syntax Description

This command has no arguments or keywords.

Command Default

Constant-carrier mode, where Data Carrier Detect (DCD) is held constant and asserted by the DCE half-duplex interface.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command applies only to low-speed serial DCE interfaces in half-duplex mode. Configure a serial interface for half-duplex mode by using the **half-duplex** command. Refer to the *CiscoProductCatalog* for specific model numbers of networking devices which support serial interfaces.

Controlled-carrier operation means that the DCE interface has DCD deasserted in the quiescent state. When the interface has something to transmit, it asserts DCD, waits a user-configured amount of time, then starts the transmission. When the interface has finished transmitting, it waits a user-configured amount of time and then deasserts DCD.

Examples

The following examples place the interface in controlled-carrier mode and then back into constant-carrier operation.

This example shows changing to controlled-carrier mode from the default of constant-carrier operation:

```
Router(config)# interface serial 2
Router(config-if)# half-duplex controlled-carrier
```

This example shows changing to constant-carrier operation from controlled-carrier mode:

```
Router(config)# interface serial 2
Router(config-if)# no half-duplex controlled-carrier
```

Related Commands

Command	Description
half-duplex	Specifies half-duplex mode on an SDLC interface or single-mode and multimode port adapters.
half-duplex timer	Tunes half-duplex timers.
physical-layer	Specifies the mode of a slow-speed serial interface on a router as either synchronous or asynchronous.

half-duplex timer

To tune half-duplex timers, use the **half-duplextimer** command in interface configuration mode. To return to the default parameter values, use the **no** form of this command.

half-duplex timer {**cts-delay** *value* | **cts-drop-timeout** *value* | **dcd-drop-delay** *value* | **dcd-txstart-delay** *value* | **rts-drop-delay** *value* | **rts-timeout** *value* | **transmit-delay** *value*}
no half-duplex timer {**cts-delay** *value* | **cts-drop-timeout** *value* | **dcd-drop-delay** *value* | **dcd-txstart-delay** *value* | **rts-drop-delay** *value* | **rts-timeout** *value* | **transmit-delay** *value*}

Syntax Description

cts-delay *value*	Specifies the delay introduced by the DCE interface from the time it detects the Request to Send (RTS) to the time it asserts Clear to Send (CTS) in response. The range is dependent on the serial interface hardware. The default **cts-delay** value is 0 ms.
cts-drop-timeout *value*	Determines the amount of time a DTE interface waits for CTS to be deasserted after it has deasserted RTS. If CTS is not deasserted during this time, an error counter is incremented to note this event. The range is from 0 to 1,140,000 ms (1140 seconds). The default **cts-drop-timeout** value is 250 ms.
dcd-drop-delay *value*	Applies to DCE half-duplex interfaces operating in controlled-carrier mode (see the **half-duplexcontrolled-carrier** command). This timer determines the delay between the end of transmission by the DCE and the deassertion of Data Carrier Detect (DCD). The range is from 0 to 4400 ms (4.4 seconds). The default **dcd-drop-delay** value is 100 ms.
dcd-txstart-delay *value*	Applies to DCE half-duplex interfaces operating in controlled-carrier mode. This timer determines the time delay between the assertion of DCD and the start of data transmission by the DCE interface. The range is from 0 to 1,140,000 ms (1140 seconds). The default **dcd-txstart-delay** value is 100 ms.
rts-drop-delay *value*	Specifies the time delay between the end of transmission by the DTE interface and deassertion of RTS. The range is from 0 to 1,140,000 ms (1140 seconds). The default **rts-drop-delay** value is 3 ms.
rts-timeout *value*	Determines the number of milliseconds the DTE waits for CTS to be asserted after the assertion of RTS before giving up on its transmission attempt. If CTS is not asserted in the specified amount of time, an error counter is incremented. The range is dependent on the serial interface hardware. The default **rts-timeout** value is 3 ms.
transmit-delay *value*	Specifies the number of milliseconds a half-duplex interface will delay the start of transmission. In the case of a DTE interface, this delay specifies how long the interface waits after something shows up in the transmit queue before asserting RTS. For a DCE interface, this dictates how long the interface waits after data is placed in the transmit queue before starting transmission. If the DCE interface is in controlled-carrier mode, this delay shows up as a delayed assertion of DCD. This timer enables the transmitter to be adjusted if the receiver is a little slow and is not able to keep up with the transmitter. The range is from 0 to 4400 ms (4.4 seconds). The default**transmit-delay** value is 0 ms.

Command Default

The default **cts-delay** value is 0 ms. The default **cts-drop-timeout** value is 250 ms. The default **dcd-drop-delay** value is 100 ms. The default **dcd-txstart-delay** value is 100 ms. The default **rts-drop-delay** value is 3 ms. The default **rts-timeout** value is 3 ms. The default**transmit-delay** value is 0 ms.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Tuning Half-Duplex Timers

The **half-duplextimer** command is used to tune half-duplex timers. With these timer tuning commands you can adjust the timing of the half-duplex state machines to suit the particular needs of their half-duplex installation.

You can configure more than one option using this command, but each option must be specified as a separate command.

Note The **half-duplextimercts-delay** command replaces the **sdlccts-delay** command. The **half-duplextimerrts-timeout** command replaces the **sdlcrts-timeout** command.

Value Ranges

The range of values for the **cts-delay** and **rts-timeout** keywords are dependent on the serial interface hardware.

Examples

The following example set the cts-delay timer to 10 ms and the transmit-delay timer to 50 ms:

```
Router(config)# interface serial 2
Router(config-if)# half-duplex timer cts-delay 10
Router(config-if)# half-duplex timer transmit-delay 50
```

Related Commands

Command	Description
half-duplex controlled-carrier	Places a low-speed serial interface in controlled-carrier mode, instead of constant-carrier mode.
physical-layer	Specifies the mode of a slow-speed serial interface on a router as either synchronous or asynchronous.

history (interface)

To enable an interface to maintain utilization history, use the **history** command in interface configuration mode. To disable an interface, use the **no** form of this command.

history {**bps** | **pps**} [*filter*]
no history

Syntax Description

bps	Maintains history in bits per second.
pps	Maintains history in packets per second.
filter	(Optional) Interface counters. See the table below for details. Any number of counters can be used.

Command Default

Interface utilization history is not maintained.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)XNE	This command was introduced.

Usage Guidelines

Once interface history is configured, the interface history histograms can be displayed using the **show interface history** command.

Some of the interface counters are interface-type-specific and cannot be specified unless they apply to the specific interface type being configured. Once interface history is configured, counters cannot be added or removed without first removing the interface history configuration.

Significant processor memory is allocated to maintain the history information. For example, if two counters are monitored, then approximately 4KB are used for the rate and counter history. If 20 counters are monitored, then approximately 19KB are used.

The table below lists the interface counter options for the **history (interface)** command.

Table 17: Interface Counter Options For Interface History

Interface Counter	Description
all	Includes all interface counters in the history.
babbles	Includes the Ethernet output babbles in the history.
crcs	Includes CRC counter in the history.
deferred	Includes the deferred Ethernet output in the history.
dribbles	Includes dribble counter in the history.
excessive-collisions	Includes Ethernet excessive output collisions in the history.
flushes	Includes flushes counter in the history.

Interface Counter	Description
frame-errors	Includes frame errors in the history.
giants	Includes giants counter in the history.
ignored	Includes ignored counter in the history.
input-broadcasts	Includes input broadcasts in the history.
input-drops	Includes input drops in the history.
input-errors	Includes input errors in the history.
interface-resets	Includes interface resets in the history.
late-collisions	Includes Ethernet late output collisions in the history.
lost-carrier	Includes Ethernet output lost carrier in the history.
multi-collisions	Includes Ethernet multiple output collisions in the history.
multicast	Includes Ethernet input multicast in the history.
no-carrier	Includes Ethernet output no-carrier in the history.
output-broadcasts	Includes output broadcasts in the history.
output-buffer-failures	Includes output buffer failures in the history.
output-buffers-swapped-out	Includes output buffers swapped out in the history.
output-drops	Includes output drops in the history.
output-errors	Includes output errors in the history.
output-no-buffer	Includes output no buffer in the history.
overruns	Includes overruns in the history.
pause-input	Includes Ethernet input pause in the history.
pause-output	Includes Ethernet output pause in the history.
runts	Includes runts in the history.
single-collisions	Includes Ethernet single output collisions in the history.
throttles	Includes throttles in the history.
underruns	Includes underruns in the history.
unknown-protocol-drops	Includes unknown protocol drops in the history.
watchdog	Includes Ethernet output watchdog in the history.

Examples

The following example shows how to configure the interface history command to maintain interface utilization history in bits per second (bps) and also the input-drop history:

```
Device(config-if)# history bps input-drops
```

Related Commands

Command	Description
show interface history	Displays information on the interface utilization.

hold-queue

To limit the length of the IP output queue on an interface, use the **hold-queue** command in interface configuration or template configuration mode. To restore the default values, use the **no** form of this command.

hold-queue *length* {**in** | **out**}
no hold-queue *length* {**in** | **out**}

Syntax Description

length	Integer that specifies the maximum number of packets in the queue. The range of valid values is from 0 to 65535.
in	Specifies the input queue. The default is 75 packets. For asynchronous interfaces, the default is 10 packets.
out	Specifies the output queue. The default is 40 packets. For asynchronous interfaces, the default is 10 packets.

Command Default

Input hold-queue limit is 75 packets. Output hold-queue limit is 40 packets. Asynchronous interfaces default is 10 packets.

Command Modes

Interface configuration (config-if)

Template configuration (config-template)

Command History

Release	Modification
10.0	This command was introduced.
11.1	The **nohold-queue**command was added.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.
15.1(2)T	This command was modified. The *length* argument was added to the **no** form of the command.
15.2(2)E	This command was integrated into Cisco IOS Release 15.2(2)E. This command is supported in template configuration mode.
Cisco IOS XE Release 3.6E	This command was integrated into Cisco IOS XE Release 3.6E. This command is supported in template configuration mode.

Usage Guidelines

Defaults

The default limits for this command prevent a malfunctioning interface from consuming an excessive amount of memory. There is no fixed upper limit to a queue size.

Back-to-Back Routing Updates

The default of 10 packets allows the Cisco IOS software to queue a number of back-to-back routing updates. This is the default for asynchronous interfaces only; other media types have different defaults.

Hold Queues and Priority Queueing

- The hold queue stores packets received from the network that are waiting to be sent to the client. Cisco recommends that the queue length not exceed10 packets on asynchronous interfaces. For most other interfaces, queue length should not exceed 100.
- The input hold queue prevents a single interface from flooding the network server with too many input packets. Further input packets are discarded if the interface has too many input packets outstanding in the system.
- If you are using priority output queueing, the length of the four output queues is set using the **priority-list** global configuration command. The **hold-queue** command cannot be used to set an output hold queue length in this situation.
- For slow links, use a small output hold-queue limit to prevent storing packets at a rate that exceeds the transmission capability of the link.
- For fast links, use a large output hold-queue limit. A fast link may be busy for a short time (and require the hold queue) but can empty the output hold queue quickly when capacity returns.
- You can display the current hold-queue setting and the number of packets that are discarded because of hold-queue overflows by using the **showinterfaces** command in user EXEC mode.

Caution Increasing the hold queue can have detrimental effects on network routing and response times. For protocols that use seq/ack packets to determine round-trip times, do not increase the output queue. Dropping packets instead informs hosts to slow down transmissions to match available bandwidth. This is generally better than having duplicate copies of the same packet within the network (which can happen with large hold queues).

Note When you use the **no** form of the **hold-queue** command, the *length* value (maximum number of packets in the queue) need not necessarily be the same as the configured value.

Examples

The following example shows how to set a small input queue on a slow serial line:

```
Router(config)# interface serial 0
Router(config-if)# hold-queue 30 in
```

The following example shows how to set an input value in an interface template:

```
Device# configure terminal
Device(config)# template user-template1
Device(config-template)# hold-queue 30 in
Device(config-template)# end
```

Cisco uBR10012 Universal Broadband Router

The following example shows how to modify the input hold queue on a Gigabit Ethernet SPA:

```
Router# configure terminal

Router(config)#interface GigabitEthernet3/0/0
Router(config-if)#hold-queue 30 in
```

Related Commands

Command	Description
priority-list	Establishes queueing priorities based on the protocol type.
show interfaces	Displays statistics for all interfaces configured on the router or access server.

hssi external-loop-request

To allow the router to support a CSU/DSU that uses the loopback circuit (LC) signal to request a loopback from the router, use the **hssiexternal-loop-request** command in interface configuration mode. To disable this function, use the **no** form of this command.

hssi external-loop-request
no hssi external-loop-request

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The HSA applique on the High-Speed Serial Interface (HSSI) contains an LED that indicates the loopback circuit A (LA), loopback circuit B (LB), and LC signals that are transiting through the devices. The CSU/DSU uses the LC signal to request a loopback from the router. The CSU/DSU may want to do this so that its own network management diagnostics can independently check the integrity of the connection between the CSU/DSU and the router.

Use this command to enable a two-way, internal, and external loopback request on the HSSI from the CSU/DSU.

Caution If your CSU/DSU does not support this function, it should not be enabled on the router. Not enabling this function prevents spurious line noise from accidentally tripping the external loopback request line, which would interrupt the normal data flow.

Examples

The following example enables a CSU/DSU to use the LC signal to request a loopback from the router:

```
Router(config-if)# hssi external-loop-request
```

hssi internal-clock

To convert the High-Speed Serial Interface (HSSI) into a clock master, use the **hssiinternal-clock** command in interface configuration mode. To disable the clock master mode, use the **no** form of this command.

hssi internal-clock
no hssi internal-clock

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command in conjunction with the HSSI null-modem cable to connect two Cisco routers together with HSSI. You must configure this command at both ends of the link, not just one.

Note HSSI network module provides full-duplex connectivity at SONET OC-1/STS-1 (51.840 Mhz), T3 (44.736 MHZ), and E3 (34.368 MHz) rates in conformance with the EIA/TIA-612 and EIA/TIA-613 specifications. The actual rate of the interface depends on the external data service unit (DSU) and the type of service to which it is connected.

Examples

The following example shows how to convert the HSSI interface into a clock master:

```
Router(config-if)# hssi internal-clock
```

hub

To enable and configure a port on an Ethernet hub of a Cisco 2505 or Cisco 2507 router, use the **hub** command in global configuration mode.

hub ethernet *number port* [*end-port*]

Syntax Description

ethernet	Indicates that the hub is in front of an Ethernet interface.
number	Hub number, starting with 0. Because there is only one hub, this number is 0.
port	Port number on the hub. On the Cisco 2505 router, port numbers range from 1 to 8. On the Cisco 2507 router, port numbers range from 1 to 16. If a second port number follows, then this port number indicates the beginning of a port range.
end-port	(Optional) Last port number of a range.

Command Default

No hub ports are configured.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command does not have a **no** form.

Examples

The following example enables port 1 on hub 0:

```
Router# hub ethernet 0 1
Router(config-hub)# no shutdown
```

The following example enables ports 1 through 8 on hub 0:

```
Router# hub ethernet 0 1 8
Router(config-hub)# no shutdown
```

Related Commands

Command	Description
shutdown (hub)	Shuts down a port on an Ethernet hub of a Cisco 2505 or Cisco 2507 router.

hw-module boot

To specify the boot options for the module through the power management bus control register, use the **hw-moduleboot** command in privileged EXEC mode.

hw-module module *num* **boot** [*value*] {**config-register** | **eobc** | **flash** *image* | **rom-monitor**}

Syntax Description

module *num*	Specifies the number of the module to apply the command.
boot *value*	(Optional) Literal value for the module's boot option; valid values are from 0 to 15. See the “Usage Guidelines” section for additional information.
config-register	Boots using the module’s config-register value.
eobc	Boots using an image downloaded through EOBC.
flash *image*	Specifies the image number in the module’s internal Flash memory for the module’s boot option; valid values are 1 and 2.
rom-monitor	Stays in ROM-monitor mode after the module resets.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXF	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The valid values for the **boot***value* argument are as follows:

0--Specifies the module’s config-register value.

1--Specifies the first image in the Flash memory.

2--Specifies the second image in the Flash memory.

3--Stays in ROM-monitor mode after the module reset.

4--Specifies the download image through EOBC.

Examples

This example shows how to reload the module in slot 6 using the module’s config-register value:

```
Router# hw-module module 1 boot config-register
Router#
```

This example shows how to reload the module in slot 3 using an image downloaded through EOBC:

```
Router# hw-module module 1 boot eobc
Router#
```

Related Commands

Command	Description
showmodule	Displays the module status and information for all modules in the chassis.

hw-module energywise level

> **Note** Effective with Cisco IOS Releases 15.1(1)T and 15.0.1M(2), the **hw-moduleenergywiselevel** command is not available in Cisco IOS software. For more information, see the Cisco 3900 Series, 2900 Series, and 1900 Series Software Configuration Guide .

To set the energywise level on the service module (SM), internal service module (ISM), or packet voice/data module (PVDM), use the **hw-moduleenergywiselevel**command in privileged EXEC mode.

hw-module *module-type* *slot-number* **energywise** **level** *level*

Syntax Description

module-type	Specifies the type of module.
slot-number	Specifies the slot, and if applicable, the sub slot number for the module.
energywise level	Specifies the power level for each module.
level	0-10. 0 will shut the power. Any number between 1 to 10 will turn the power on.

Command Default

The energywise level is 10.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

Use the **hw-moduleenergywiselevel**command in privileged EXEC mode to set the energywise level on the SM, ISM, or PVDM on your router. Specify the slot, and if applicable, the sub slot number for the module.

The energywise levelsupported for the module is specified by the module. The following table provides a definition for each energywise level:

Energywise Level	Definition
0	Shut
1	Hibernate
2	Sleep
3	Standby
4	Ready
5	Low
6	Frugal

Energywise Level	Definition
7	Medium
8	Reduced
9	High
10	Full

Note When the router reboots, the energywise level is set to energywise level 10 and will remain at energywise level 10 till a different energywise level is applied.

Examples

The following example shows how to set the energywise level at shut on an SM in slot 1.

```
Router#hw-module
sm 1
 energywise level
0
```

The following example shows how to set the energywise level at full on an SM in slot 1.

```
Router#hw-module
sm 1
 energywise level
10
```

Related Commands

Command	Description
show environment	To display temperature, voltage, fan, and power supply information, use the **showenvironment** command in user EXEC or privileged EXEC mode.
show platform hw-module-power	To display the energywise levels supported on the module, and the current and previous energywise level on the router, use the show platform hw-module-power command in user EXEC or privileged EXEC mode.

hw-module fan-tray version

To set the fan-type (high or low power) version, use the **hw-modulefan-trayversion**command in privileged EXEC mode.

hw-module fan-tray version [{**1** | **2**}]

Syntax Description

1 | 2	(Optional) Specifies the version number; see the “Usage Guidelines” section for additional information.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Before you install a high-capacity fan tray, enter the **hw-modulefan-trayversion2** command to check for configuration problems, such as power-supply compatbility and power sufficiency. If there are no problems, a message is displayed to change the fan tray from version 1 to version 2. At this point, you can remove the old fan tray and quickly insert the new high-capacity fan tray.

The **hw-modulefan-trayversion2** command aplies to Cisco 7600 series routers configured with a Supervisor Engine 2. This command is not required in systems configured with a Supervisor Engine 720 or a Supervisor Engine 32.

This command is supported on the following chassis:

- WS-C6506
- WS-C6509
- WS-C6509-NEB/OSR7609

Set the version to **2** before installing higher power fan trays.

Set the version to **1** before downgrading to lower power fan trays.

Command confirmation does not change the fan power consumption or cooling capacity. It updates the backplane IDPROM. The new values take effect the next time that you insert a fan.

When you execute the command, the software checks the configurations and prompts for confirmation. Any illegal configurations (such as power-supply incompatibility) result in a warning being displayed and a command failure.

Examples

This example shows how to set the fan type for lower power fan trays:

```
Router#
hw-module fan-tray version 1
```

Related Commands

Command	Description
show environment cooling	Displays information about the cooling parameter.

hw-module interface als restart

To request a restart pulse when Automatic Laser Shutdown (ALS) restart mode is configured as manual, use the **h**w-module interface TenGigabitEthernet als restart command in Privileged EXEC mode.

hw-module interface TenGigabitEthernet slot/port als restart

Syntax Description

slot/port	Number of the chassis slot that contains the interface, where:
	• slot--Chassis slot number.
	• /port--Port number.
	  • For a 7600-ES+ITU-2TG, the valid values for the port are 1, 2.
	  • For a 7600-ES+ITU-4TG, the valid values for the port are 1, 2, 3, 4.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRD1	This command was introduced on the Cisco 7600 series router.

Examples

The following example shows how to request an ALS restart pulse for the Ten Gigabit Ethernet interface on slot 6 port number 2:

```
Router# hw-module interface TenGigabitEthernet 6/2 als restart
```

Related Commands

Command	Description
als	Enables the ALS mode.
als restart mode	Selects the ALS restart mode.
als restart pulse	Select the ALS pulse mode.
show als	Displays ALS status.
show controller dwdm	Displays G.709 alarms, alerts, and counters.
transport-mode	Configures a transport mode.

hw-module main-cpu qa error-recovery

To enable the recovery mechanism for a QA error condition on a Cisco 7500 series router, use the **hw-modulemain-cpuqaerror-recovery** command in global configuration mode. To disable the recovery mechanism for a QA error condition, use the **no** form of this command.

hw-module main-cpu qa error-recovery
no hw-module main-cpu qa error-recovery

Syntax Description

This command has no arguments or keywords.

Command Default

In Cisco IOS Release 12.0(24)S1, the recovery mechanism for a QA error condition is disabled; in all other releases, it is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(19)E	This command was introduced.
12.0(24)S1	This command was integrated into Cisco IOS Release 12.0(24)S1.
12.2(15)T5	This command was integrated into Cisco IOS Release 12.2(15)T5.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.3(6)	This command was integrated into Cisco IOS Release 12.3(6).

Usage Guidelines

QA errors are sometimes seen in heavy traffic situations and may indicate a hardware failure or a software bug. In the case of a hardware failure, a Versatile Interface Processor (VIP) or a Route Switch Processor (RSP) must be replaced. It is possible, however, to recover from a QA error and not see another error for months. When the same buffer header is present in two different queues, the QA ASIC goes into an error condition and triggers a QA error interrupt. The QA error interrupt causes the RSP to dump the QA diagnostics and perform a cbus complex during which all the line cards are reloaded. Although the duplicate buffer header condition does not always indicate a hardware failure, the downtime of up to 300 seconds creates a real problem in the network.

The **hw-modulemain-cpuqaerror-recovery** command has been created to enable a recovery mechanism for a QA error by allowing the router to remove the duplicate buffer header from the queue that shows the problem and requeue the buffer header. By using the QA error recovery, the downtime is reduced to less than one second under lab conditions. Three QA errors caused by buffer headers are permitted before the router performs a cbus complex and reloads all the line cards.

After three QA errors caused by duplicate queued buffer headers occur, the cbus complex is initiated and the line cards reload. Other QA errors, such as a null buffer header on any queue, can occur. Recovery is not possible in these cases, and the QA error triggers a cbus complex and subsequent line-card reloads. The QA error condition is specific to the Cisco 7500 series routers.

Examples

The following example shows how to enable the QA error recovery mechanism when a Cisco IOS Release 12.0(24)S1 image is used on a Cisco 7500 series router. In all other supported releases, the QA error recovery mechanism is enabled by default.

```
Router(config)# hw-module main-cpu qa error-recovery
```

Related Commands

Command	Description
show controllers cbus	Displays information about the cBus controller card.

hw-module mode

To configure the interface module from 10G to 5G mode, use the **hw-module mode** command in global configuration mode.

hw-module *slot* / *bay PID***mode** *mode*

Use the following command to disable the eight unused odd ports (1, 3, 5, 7, 9, 11, and 15) of A900-IMA8CS1Z-M interface modules within the slots of Cisco N560-RSP4 and Cisco N560-RSP4-E routers:

hw-module *slot 0-15* **im-mode** *1*

Syntax Description

Syntax Description:

slot	Physical slot number of the interface
bay	Bay of the interface
PID	Part number of the interface modules
mode	Option to select the mode of the interface module
mode	Selected mode of the Interface Module, for example 5G_CEM.

Command Default

Default is 10G mode

Command Modes

Global configuration

Command History

Release	Modification
XE Everest 16.5.1	This command was introduced into the Cisco NCS 4200 Series, NCS 560 Series, and Cisco ASR 900 Series Routers.

Usage Guidelines

We recommend that you remove all the configurations before configuring 5G mode for the interface module. Do not use the **mode** keyword if you want to configure 10G mode.

Note Only 4-port-only mode is supported on the 8-port 10 Gigabit Ethernet Interface Module (8x10GE) interface module.

Examples

The following example shows how to configure configure 5G mode from 10G mode:

```
enable
configure terminal
platform hw-module configuration
hw-module 0 / 3 PID mode 5G_CEM
end
```

The following example shows the configuration of 8-port 10 Gigabit Ethernet Interface Module (8x10GE) interface module:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# platform hw-module configuration
Router(conf-plat-hw-conf)# hw-module 0/3 A900-IMA8Z mode ?
  4-ports-only  Four Ports

Router(conf-plat-hw-conf)#hw-module 0/3 A900-IMA8Z mode 4-ports-only

Interface configs would be defaulted before mode change?? [yes/no]: yes
```

Related Commands

Command	Description
show running-config | include mode	Verifies if the interface module is configured in 5G mode.

hw-module oversubscription

To administratively disable the oversubscribed ports (3, 4, 7, and 8) on a module, use the **hw-moduleoversubscription** command. Use the **no** form of this command to enable the oversubscribed ports.

hw-module module *num* **oversubscription**
no hw-module module *num* **oversubscription**

Syntax Description

module *num*	Applies the command to a specific module.

Command Default

Oversubscription is enabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced (Cisco 76700 series router).
12.2(18)SXF5	Support for this command was intruduced (Catalyst 6500 series switch).

Usage Guidelines

This command is supported on the WS-X6708-10G-3C and the WS-X6708-10G-3CXL modules only.

When you disable the oversubscribed ports, the port is put into shutdown mode. In this mode, you cannot enter the **noshut** command on the disabled ports. If you attempt to enter the **noshut** command on the disabled ports, this message appears:

```
The current module is operating in non-oversubscription mode. To utilise this interface,
enable oversubscription mode for the module.
```

When you enter the **showinterfaces** command on the disabled ports, the output displays “disabled for performance” to distinguish between the normal port shutdown and the shutdown for performance.

Examples

This example shows how to administratively disable the oversubscribed ports on a module:

```
Router #
hw-module module 3 oversubscription
Router #
```

This example shows how to administratively enable the oversubscribed ports on a module:

```
Router #
no hw-module module 3 oversubscription
Router #
```

Related Commands

Command	Description
show interfaces	Displays traffic that is seen by a specific interface.

hw-module power-supply power-cycle

To power cycle the power supplies, use the **hw-modulepower-supplypower-cycle**command in privileged EXEC mode.

hw-module power-supply {**1** | **2**} **power-cycle**

Syntax Description

1 | **2**	Specifies the power supply to power cycle.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)SXF	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If you have redundant power supplies and you power cycle one of the power supplies, only that power supply is power cycled. If you power cycle both power supplies, the system goes down and comes back up in 10 seconds.

If you only have one power supply and you power cycle that power supply, the system goes down and comes back up in 10 seconds.

This command works only on routers with an 8700 watt power supply.

Examples

This example shows how to power cycle a power supply:

```
Router# hw-module power-supply 2 power-cycle
Power-cycling the power supply may interrupt service.
Proceed with power-cycling? [confirm]
Power-cycling power-supply 1
22:10:23: %C6KPWR-SP-2-PSFAIL: power supply 1 output failed.
22:10:25: %C6KENV-SP-4-PSFANFAILED: the fan in power supply 1 has failed
22:10:33: %C6KPWR-SP-4-PSOK: power supply 1 turned on.
22:10:33: %C6KENV-SP-4-PSFANOK: the fan in power supply 1 is OK
Router#
```

hw-module pxf stall-monitoring

To enable the parallel express forwarding (PXF) stall monitor on the Cisco 10000 series router, and configure the default threshold values for resetting the line card (LC) and the Hyper Transport Data Protocol (HTDP), use the **hw-modulepxfstall-monitoring**command in the global configuration mode. To disable the PXF stall monitor, use the **no** form of this command.

hw-module pxf stall-monitoring [{**HT-Reset** *threshold-value* | **LC-Reset** *threshold-value*}]
no hw-module pxf stall-monitoring [{**HT-Reset** *threshold-value* | **LC-Reset** *threshold-value*}]

Syntax Description

HT-Reset *threshold-value*	Specifies the threshold value for HTDP reset. The valid value ranges from 4 to 6. By default, the threshold value is set to 3.
LC-Reset *threshold-value*	Specifies the threshold value for LC reset. The valid value ranges from 4 to 6. By default, the threshold value is set to 3.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)XNE	This command was introduced.

Usage Guidelines

Initially, use the **hw-modulepxfstall-monitoring**command to enable the PXF stall monitor on the Cisco 10000 series router. Then use the **hw-modulepxfstall-monitoring**command again, to configure the threshold values of LC and HTDP reset.

Examples

The following example shows how to enable the PXF stall monitor, and configure the threshold values of LC and HTDP reset, using the **hw-modulepxfstall-monitoring**command.

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# hw-module pxf stall-monitoring
Router(config)# hw-module pxf stall-monitoring HT-Reset 5
Router(config)# hw-module pxf stall-monitoring LC-Reset 4
```

Related Commands

Command	Description
show pxf stall-monitoring	Displays the current configuration and the operating status of the PXF stall monitor.

hw-module reset

To reset a module by turning the power off and then on, use the **hw-module reset** command in privileged EXEC mode.

hw-module module *num* **reset**

Syntax Description

module *num*	Applies the command to a specific module; see the "Usage Guidelines" section for valid values.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	This command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS 12.2(31)SB2.

Usage Guidelines

The *num* argument designates the module number. Valid values depend on the chassis that is used. For example, if you have a 13-slot chassis, valid values for the module number are from 1 to 13.

Examples

This example shows how to reload a specific module:

```
Router#
hw-module module 3 reset
```

hw-module sec-cpu reset

To reset and reload the standby Route Switch Processor (RSP) with the specified Cisco IOS image and to execute the image, use the **hw-modulesec-cpureset** command in privileged EXEC mode.

hw-module sec-cpu reset

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(16)ST	This command was introduced.
12.0(19)ST1	This command was enabled in privileged EXEC mode.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(4)XF	This command was integrated into Cisco IOS Release 12.2(4)XF on the Cisco uBR10012 router.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.3BC	This command was integrated into Cisco IOS Release 12.3BC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Before using this command, you must use the **hw-moduleslotimage**global configuration command to specify a high availability Cisco IOS image to run on the standby RSP. After the high availability image is loaded in the active RSP, use the **hw-modulesec-cpureset** command to reset and reload the standby RSP with the specified Cisco IOS image and to execute the image. To load the standby RSP with the default micro-IOS software contained in the active RSP image instead of a high availability Cisco IOS image, use the **no** form of the **hw-moduleslotimage** command followed by the **hw-modulesec-cpureset**command.

Examples

The following example shows a Cisco 7513 router with the standby RSP loaded in slot 7. The standby RSP is reset and reloaded with the rsp-pv-mz high availability Cisco IOS image. Both RSPs have slot 0 flash memory cards.

```
Router(config)# hw-module slot 7 image slot0:rsp-pv-mz
Router(config)# end
Router# hw-module sec-cpu reset
```

Related Commands

Command	Description
hw-module slot image	Specifies a high availability Cisco IOS image to run on an active or standby RSP.

hw-module shutdown

To shut down the module, use the **hw-module shutdown** command in privileged EXEC mode.

hw-module module *num* **shutdown**

Syntax Description

module *num*	Applies the command to a specific module; see the "Usage Guidelines" section for valid values.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported on the SSL Services Module and the NAM.

If you enter the hw-module **shutdown**command to shut down the module, you will have to enter the no power enable module command and the **power enable module** command to restart (power down and then power up) the module.

Examples

This example shows how to shut down and restart the module:

```
Router# hw-module module 3 shutdown
Router# no power enable module 3
Router# power enable module 3
```

hw-module simulate link-up

To enable softlink on a specified module, use the **hw-modulesimulatelink-up**command in privileged EXEC mode. For information on disabling softlink, refer to the "Usage Guidelines" section.

hw-module module *num* **simulate link-up**

Syntax Description

module *num*	Applies the command to a specific module; see the "Usage Guidelines" section for valid values.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 720 and the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported on Ethernet modules only.

To disable softlink on a module, you must perform one of the following procedures:

- Enter the **shutdown** and then the **noshutdown**commands on all the ports on the module.
- Enter the **hw-modulereset**command.

When you apply this command to a module, the port LEDs on the module will glow green and simulate a link-up condition. This command can be used for testing interface configurations without cabling to the interface.

The *num* argument designates the module number. Valid values depend on the chassis that is used. For example, if you have a 13-slot chassis, valid values for the module number are from 1 to 13.

Examples

This example shows how to enable softlink on a module:

```
Router# hw-module module 3 simulate link-up
Router#
```

Related Commands

Command	Description
hw-module reset	Resets a module by turning the power off and then on.

hw-module slot

T o enable the router shelf to restart a stopped Dial Shelf Controller (DSC) card, to stop a DSC card, or to cause a shutdown, reset, or reload of any specified dial shelf feature board, use the **hw-moduleslot**command in privliged EXEC mode and global configuration mode.

hw-module slot *shelf-id/slot-number* {**reload** | **reset** | **shutdown** {**powered** | **unpowered**} [**dual-wide**] | **start** | **stop**}

Syntax Description

shelf-id	Number of the dial shelf. The default number for the dial shelf is 1.
/ *slot-number*	Number of the slot in the shelf where the target feature board or DSC is installed. If the **start** or **stop** keyword is used, the slot number must be either 12 or 13, because these keywords apply only to DSCs.
reload	Enables a remote reload of an individual feature board without having to use manual online insertion and removal (OIR).
reset	Resets a feature board.
shutdown	Shuts down a feature board.
powered	Shuts down the DSC and all of its interfaces and leaves them in an administratively down state with power enabled.
unpowered	Shuts down the DSC and all of its interfaces and leaves them in an administratively down state without power.
dual-wide	(Optional) Specifies the dual-wide port adapter (PA).
start	Restarts the specified DSC.
stop	Stops the specified DSC.

Command Default

Shuts down the DSC and all of its interfaces and leaves them in an administratively down state with power enabled.

Command Modes

Global configuration (config) Privileged EXEC (#)

Command History

Release	Modification
11.3(6)AA	The **hw-module** command was introduced.
12.1	• The **hw-module** command was expanded to become the **hw-moduleslot**command. • The **reload** keyword was added to enable a remote reload of a feature board.
12.3(2)T	The**reset**and **shutdown** keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SB	This command's behavior was modified on the Cisco 10000 series router for the PRE3 and PRE4, and the **reload** option was introduced on the router.
15.0(1)M	This command was modified. The command became available in global configuration mode. The **powered**, **unpowered**, and **dual-wide** keywords were added.

Usage Guidelines

The **stop** form of this command is issued from the router shelf console instead of by pressing the attention (ATTN) button on the target DSC. Confirmation of when the start or stop took place is displayed. Warnings are issued and confirmation input is required if a **stop** command will result in a loss of service when backup functionality is not available.

When a DSC card is stopped, removed, and then reinstalled, there is no need to restart the card (whether the card is the original or a replacement) because a freshly installed card reboots as the backup DSC automatically. However, if a DSC is stopped, either by using the ATTN button or by issuing the **hw-moduleslotstop** command, it must be restarted by using the **start** form of the same command, or the DSC must be removed and reinstalled in order to reboot.

Press the ATTN button on the DSCs to shut down a card manually before removing the card. This is equivalent to issuing an **hw-moduleslot** command for that card at the router command prompt. Use the ATTN button to shut down the card before it is swapped out or tested in place, or to restart it, if the card has not been removed after having been shut down.

Tip The **hw-module** slot *shelf-id*/*slot-number***reload** form of this command is useful for simulating an OIR event in the case of a feature board failure when physical access to the feature board card is restricted.

Entering the **hw-module** slot *shelf-id*/*slot-number***reload**command initiates the feature board reload process through power cycling. The **hw-module** slot *shelf-id*/*slot-number***reload** command cannot be used to reload DSCs.

Use the **reset** form of this command to reset the specified feature card and drop all active calls.

Use the **shutdown** form of this command to shut down the specified feature card and drop all active calls.

Cisco 10000 Series Router Usage Guidelines,

In Cisco IOS Release 12.2(33)SB, when you enter the **hw-moduleslot***slot-number***reset** command, the software asks you to confirm the command.

In Cisco IOS Release 12.2(31)SB, the software does not ask you to confirm the **hw-moduleslot***slot-number***reset** command.

Examples

The following example shows how to stop the DSC in slot 13 and start the other DSC in slot 12 (which was previously stopped):

```
Router# hw-module slot 1/13 stop
Router# hw-module slot 1/12 start
```

The following example shows how to reload the dial shelf feature board in slot 6:

```
Router# hw-module slot 1/6 reload
```

The following example shows how to reset the card in slot 3:

```
Router# hw-module slot 1/3 reset
```

The following example shows how to shut down the PRE card located in slot 3:

```
Router# hw-module slot 1/3 shutdown powered
```

Related Commands

Command	Description
debug redundancy	Displays information used for troubleshooting dual (redundant) DSC cards.
show redundancy	Displays current or historical status and related information on dual (redundant) DSC cards.

hw-module slot (6500)

To enable ports on a module, use the **hw-moduleslot** command. To disable ports on a module, use the **no** form of this command.

hw-module slot *num* {**clear-block** | **oversubscription**} [**port-group** *num*]
no hw-module slot *num* {**clear-block** | **oversubscription**} [**port-group** *num*]

Syntax Description

slot *num*	Applies the command to a specific module.
clear-block	Drops the packets that are destined for jammed ports and continues delivering the packets for other ports.
oversubscription	Administratively disables the oversubscribed ports on a module. To enable oversubscription, use the **no** form of this command.
port-group *num*	(Optional) Applies the command to a specific port group on the module. The range depends on the module type.

Command Default

The default settings are as follows:

- Clear block is enabled by default.
- Oversubscription is enabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXF5	Support for this command was introduced (Catalyst 6500 series switch).
12.2(33)SXH1	Support for these keywords and arguments were introduced: • clear-block [port-group *num* • oversubscription [port-group *num*
12.2(33)SXH2	This command was changed to support the following modules: • WS-X6716-10G-3C • WS-X6716-10G-3CXL

Usage Guidelines

This command is supported on the following modules:

- WS-X6708-10G-3C--The port-group *num* and the clear-block keywords and argument are not supported.
- WS-X6708-10G-3CXL--The port-group *num* and the clear-block keywords and argument are not supported.
- WS-X6716-10G-3C

- WS-X6716-10G-3CXL

When you disable the oversubscribed ports, the port is put into shutdown mode. In this mode, you cannot enter the **noshut** command on the disabled ports. If you enter the **noshut** command on the disabled ports, this message appears:

```
The current module is operating in non-oversubscription mode. To utilise this interface,
enable oversubscription mode for the module.
```

When you enable oversubscription for a port group, the port group is in mux mode. When you disable oversubscription, the port group is in transparent mode. When a group is in transparent mode, the first port in the group retains its administrative status and the remaining three ports are administratively shut down. You cannot enter the **shut**, and then the **noshut** commands on the disabled ports. You can enter the **shut**, and then the **noshut** commands on the enabled port in the group.

The port-group mappings for the WS-X6716-10G-3C and the WS-X6716-10G-3CXL modules are as follows:

- Group 1--Ports 1 to 4. Port 1 is enabled in transparent mode.
- Group 2--Ports 5 to 8. Port 5 is enabled in transparent mode.
- Group 3--Ports 9 to 12. Port 9 is enabled in transparent mode.
- Group 4--Ports 13 to 16. Port 13 is enabled in transparent mode.

For the WS-X6716-10G-3C and the WS-X6716-10G-3CXL modules in transparent mode, ports 2, 3, 4, 6, 7, 8, 10, 11, 12, 14, 15, 16 are disabled.

If you specify a slot number without a group number, all four groups are put into transparent/mux mode.

You cannot put the port group into oversubscription mode when any port in the port group is configured as a virtual switch link (VSL). A warning message is displayed asking you to disable the VSL link before changing to oversubscription mode.

When you enter the **showinterfaces** command on the disabled ports, the output displays “disabled for performance” to distinguish between the normal port shutdown and the shutdown for performance.

Each 4-port group shares a common packet queue. If head-of-line blocking is enabled and one port of the four ports receives a pause frame, all packets are blocked behind this packet until the packet is delivered to the flow-controlled port. You can enter the **hw-moduleslot**clear-block [port-group *num*] command to drop the packets that are destined for the jammed port and continue to deliver the packets for other ports.

Examples

This example shows how to administratively disable the oversubscribed ports on a module:

```
Router#
no hw-module slot 3 oversubscription
Router#
```

This example shows how to administratively disable the oversubscribed ports on a specific port group:

```
Router#
no hw-module slot 3 oversubscription port-group 4
Router#
```

This example shows how to administratively enable the oversubscribed ports on a module:

```
Router#
hw-module slot 3 oversubscription
Router#
```

This example shows how to drop the packets that are destined for the jammed port and continue to deliver the packets for other ports:

```
Router#
hw-module slot 3 clear-block port-group 4
Router#
```

Related Commands

Command	Description
show interfaces	Displays traffic that is seen by a specific interface.
show hw-module slot	Displays information for a SPA interface processor (SIP) or other module.

hw-module slot (7300)

To prepare a line card, MSC, or PCI port adapter carrier card for online removal, use the**hw-moduleslot** command in privileged EXEC mode.

hw-module slot *slot-number* {**stop** | **start**}

Syntax Description

slot-number	Specifies the slot number of the line card, MSC, or PCI port adapter carrier card.
stop	Stops traffic, turns on the OIR LED, shuts down all interfaces, and deactivates the line card, MSC, or PCI port adapter carrier card.
start	Restarts the line card and shuts off the OIR LED, putting the hardware back online.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(9)EX	This command was enabled on the Cisco 7304 router.
12.2(18)S	This command was introduced on Cisco 7304 routers running Cisco IOS Release 12.2(18)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **hw-moduleslot***slot-number***stop**command to stop traffic, turn on the green OIR LED, and shut down all interfaces to remove a line card, MSC, or PCI port adapter carrier card from the Cisco 7304 router without disrupting data flow. You should not remove hardware while traffic is still running.

The **stop** keyword stops traffic through interfaces and deactivates the hardware. When the OIR LED turns green, the hardware has been deactivated and can be physically removed.

The **hw-moduleslot***slot-number***start**command restarts the line card, MSC, or PCI port adapter carrier card and shuts off the OIR LED, putting the card back online.

Use the **hw-moduleslot***slot-number***start**command if you issue the **hw-moduleslot***slot-number***stop** command, did not remove the hardware, and now want to reactivate it. If you remove and then reinsert the hardware, the hardware restarts without this command.

This command cannot be used for online removal of SPAs. For online removal of SPAs, use the **hw-modulesubslot** command.

You can also use thiscommand to restore a line card, MSC, or PCI port adapter carrier card that has been deactivated due to some failure.

> **Note** Line cards, MSCs, and PCI port adapter carrier cards are automatically initialized after being inserted or after a system bootup. You do not need to issue the**hw-moduleslot***slot-number***start** command.

Examples

The following example shows how to deactivate the line card, MSC, or PCI port adapter carrier card in slot 2. After entering this command and the green OIR LED turns on, you can remove the hardware and insert a new piece of hardware:

```
Router# hw-module slot 2 stop
```

The following example shows how to reactivate a line card, MSC, or PCI port adapter carrier card in slot 2. You only need to enter this command if you enter the **hw-moduleslot** *slot-number***stop** command but do not remove the hardware and instead want to restart the hardware.

```
Router# hw-module slot 2 start
```

Related Commands

Command	Description
hw-module subslot	Prepares a SPA for online removal.
show c7300	Displays the types of cards (NSE and line cards) installed in a Cisco 7304 router.
show diag	Displays hardware information for any slot or the chassis.
show c7300 errorlog	Displays error information on a Cisco 7304 series router.
show platform errorlog	Displays error information for any installed card.

hw-module slot (7600)

To enable ports on a module, use the **hw-module slot** command in global configuration mode. To disable the ports, use the **no** form of this command.

hw-module slot *slot-number* {**memory test full** | **oversubscription** | **pos** | **process-max-time** *number-of-seconds* | **rate-limit** {**fsol_rate** *fsol-rate* | **punt_rate** *punt-packet-rate*} | **srp** | **subslot** *subslot-number* **only** | **mp-recovery-enable** | **ipv6-hbh-rl** *rate* }
no hw-module slot *slot-number* {**memory test full** | **oversubscription** | **pos** | **process-max-time** *number-of-seconds* | **rate-limit** {**fsol_rate** *fsol-rate* | **punt_rate** *punt-packet-rate*} | **srp** | **subslot** *subslot-number* **only** | **mp-recovery-enable** | **ipv6-hbh-rl** *rate* }

Syntax Description

slot-number	Chassis slot number.
memory	Specifies the memory settings of a module.
test	Specifies the memory options available for testing.
full	Performs a complete memory test on the Lower Circuit (LC).
oversubscription	Administratively disables the oversubscribed ports on a module.
pos	Converts a module to packet-over-SONET (POS) mode.
process-max-time	Specifies the maximum time for which the process runs before it stops the processor.
number-of-seconds	Number of milliseconds before the processor suspends voluntarily.
rate-limit	Limits the packets that are sent to the Route Processor (RP).
fsol_rate *fsol-rate*	Limits the broadband and Ethernet Flow Point (EFP) First Sign of Life (FSOL) packets, in bits per second (b/s). The default is 40000 b/s (or 50 packets per second for a 100-byte packet). • This keyword is specific to the ES+ line card.
punt_rate *punt-packet-rate*	Limits the Layer 4 and Port-Bundle Host Key (PBHK) packets, in bits per second (b/s). The default is 1000000 b/s. • This keyword is specific to the ES+ line card.
srp	Converts a module to Spatial Reuse Protocol (SRP) mode.
subslot *slot-number* **only**	Specifies the secondary slot number to enable a slot to support a single Shared Port Adapter (SPA).
mp-recovery-enable	Enables metropolis stuck recovery. This option is enabled by default. Use the **no** form to disable this option.

ipv6-hbh-rl *rate*	Specifies the policing rate-limit for the IPv6 Hop-by-Hop extension header packets. • For the SIP-400, you can configure a rate of up to 25600 packets per second (PPS). The default police rate is 21.36 kpps. • For the ES+ line cards, you can configure a rate of up to 100000 kbps. The default police rate is 12000 kbps.

Command Default

Ports are not enabled on a module.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)S	This command was introduced.
15.2(4)S	This command was modified. The **mp-recovery-enable** keyword was added.
12.2(33)SRE6	This command was integrated into Cisco IOS Release 12.2(33)SRE6.
12.2(33)SRE7	This command was modified. The **mp-recovery-enable** keyword was added.
15.3(1)S	This command was modified. The **ipv6-hbh-rl** keyword was added.

Usage Guidelines

- The FSOL queue is used by broadband FSOL and EFP FSOL.
- The punt queue is used by Layer 4 and PBHK packets.
- An increase in the number of either FSOL or punt rate limiters enables more packets to reach the RP. This increase exerts more load on the RP CPU. Therefore, changing the default values of either FSOL or punt rate limiters is not recommended.
- On the ES+ line cards, setting the police rate to 0 turns off the policing. On the SIP-400, the policing does not stop but all the packets are dropped.
- For both the ES+ line cards and the SIP-400, when the policer is set from the line card console, the setting remains effective even if the line card is moved to another chassis running the Cisco IOS Release 15.3(1)S or later images.
- For the SIP-400, IPv6 HBH packets continue to go through the QoS policing configured on the line card. For the ES+ line cards, IPv6 HBH packets bypass any QoS policing configured on the line card.

Examples

The following example shows how to set the FSOL rate to 50000 b/s:

```
Device(config)# hw-module slot 2 rate-limit fsol_rate 50000
```

The following example shows how to set the punt rate to 70000 b/s:

```
Device(config)# hw-module slot 2 rate-limit punt_rate 70000
```

The following example shows how to set the rate limit for the IPv6 Hop-by-Hop extension header packets to 777 kbps:

```
Device(config# hw-module slot 2 ipv6-hbh-rl 777
```

Related Commands

Command	Description
show hw-module slot	Displays system information for a SPA interface processor (SIP) or a module.

hw-module slot (ASR 1000 Series)

To start, stop, reload, or enable logging for an Embedded Services Processor (ESP), Route Processor (RP), or Shared Port Adapter (SPA) Interface Processor (SIP) on a Cisco ASR 1000 Series Aggregation Services Router, use the **hw-moduleslot** command in privileged EXEC or global configuration or diagnostic mode.

hw-module slot *slot action*

Syntax Description

slot	Slot on which logging action is to be taken. Options are as follows: • *number* --the number of the SIP slot. • **f0** --The ESP in ESP slot 0. • **f1** --The ESP in ESP slot 1 • **r0** --The RP in RP slot 0. • **r1** --The RP in RP slot 1.
action	The action to take on the hardware in the specified *slot*. Options are as follows: • **logging onboard** [**disable**| **enable**] --Disables or enables onboard logging of the hardware. • **reload** --Reloads the specified hardware. • **start** --Starts the hardware if it has been stopped. • **stop** --Stops the hardware if it is currently active.

Command Default

The router sends and receives traffic by default, so this command is not necessary to enable any hardware on a router. Onboard logging for all of the hardware is enabled by default.

Command Modes

Diagnostic (diag) Privileged EXEC (#) Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.

Usage Guidelines

The **hw-moduleslot** command does not have a **no** form.

To start, stop, or reload a SPA, use the **hw-modulesubslot**command.

The **stop** and **reload** options cannot be used on an active RP.

All traffic to hardware that has been set to stop using the **stop** option will be dropped until the hardware is reenabled by either physically removing and reinserting the hardware, or entering the **start** option. After the hardware is modified as appropriate or the **start** option is entered, the hardware has to reinitialize before it is able to send and receive traffic. Note that in some cases reinitialization can take several minutes, and that the reinitialization time required depends on the hardware and the system configuration.

When a SIP is stopped, all traffic to all SPAs in the SIP is dropped. The SPAs in the SIP can begin receiving traffic after the SIP is restarted using the **start** option and all SPAs and the SIP finish reinitializing.

Since this is a privileged EXEC-level command, this command setting cannot be saved to the startup configuration and therefore the command setting cannot be maintained after a system reload. If you want the hardware to stay in the **stop** state across system reloads, use the **hw-moduleslot***slot***shutdown** global configuration command.

The **reload** option can be used to reload hardware for any reason; for example, to finish a software upgrade that requires reloading of the hardware or to reload the hardware as part of a troubleshooting step.

The contents of onboard logging logs can be displayed using the **showloggingonboardslot** privileged EXEC and diagnostic mode commands.

Enter the **showloggingonboardslot***slot***status** privileged EXEC or diagnostic command to see if onboard logging is enabled or disabled for the hardware in a particular slot.

When the **hw-moduleslot***slot***loggingonboarddisable** command is entered, onboard logging for the specified hardware component is disabled but the existing logs are preserved; if you want to erase the existing logs, enter the **clearloggingonboardslot** command.

When the **hw-moduleslot** command is entered in global configuration mode (for ESP40 and SIP40 cards), you have a link option that allows you to choose among a set of backplane enhanced serializer/deserializer (SerDes) interconnect (ESI) links between ESP and a given SIP slot. The range of possible values for the link depends on the type of ESP and SIP cards. Only a combination of ESP40 and SIP40 cards can have more than two ESI links (link A and link B). All other cards have only link A. For example, a combination of ESP40 and SIP10 or ESP20 and SIP40 cards can have only one link (link A).

Examples

The following example shows how to stop the RP in RP slot 0:

```
Router# hw-module slot r0 stop
```

The following example shows how to disable the onboard logging for the RP in RP slot 0. The output of the **showloggingonboardslotr0status**command is given both before and after onboard logging is disabled to verify that onboard logging was properly disabled.

```
Router# show logging onboard slot r0 status

Status: Enabled
Router# hw-module slot r0 logging onboard disable
Router# show logging onboard slot r0 status

Status: Disabled
```

The following example shows how to display the available link options for ESP40 and SIP40 cards:

```
Router(config)# hw-module slot 0 qos input link ?
A  ESI Link A
B  ESI Link B
```

Related Commands

Command	Description
clear logging onboard slot	Clears the data in an onboard slot log.
hw-module subslot	Starts, stops, or reloads a SPA.

Command	Description
show logging onboard slot	Displays the status of onboard logging, or the contents of an onboard logging log.

hw-module slot image

To specify a high availability Cisco IOS image to run on an active or standby Route Switch Processor (RSP), use the **hw-moduleslotimage** command in global configuration mode. To remove a high availability Cisco IOS image from the running configuration, use the **no** form of this command.

hw-module slot *slot-number* **image** *file-spec*
no hw-module slot *slot-number* **image** *file-spec*

Syntax Description

slot-number	Specifies the number of the RSP slot.
file-spec	Specifies the flash memory card location to load the image into and the name of the image.

Command Default

No high availability Cisco IOS images are specified to run on the active or standby RSPs.

Command Modes

Global configuration

Command History

Release	Modification
12.0(16)ST	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Examples

The following example shows a Cisco 7513 router with the active RSP loaded in slot 6 and the standby RSP loaded in slot 7. The rsp-pv-mz high availability Cisco IOS image is specified to run on both the active and the standby RSP. Both RSPs have slot 0 flash memory cards.

```
Router(config)# hw-module slot 6 image slot0:rsp-pv-mz
Router(config)# hw-module slot 7 image slot0:rsp-pv-mz
```

Related Commands

Command	Description
hw-module sec-cpu reset	Resets and reloads the standby RSP with the specified Cisco IOS image and executes the image.
mode (HSA redundancy)	Configures the redundancy mode.
redundancy	Enters redundancy configuration mode.

hw-module slot subslot only

Note This command is deleted effective with Cisco IOS Release 12.2SXI.

To change the mode of the Cisco 7600 SSC-400 card to allocate full buffers to the specified subslot, use the **hw-moduleslotsubslotonly** command in global configuration mode. If this command is not used, the total amount of buffers available is divided between the two subslots on the Cisco 7600 SSC-400.

Note This command automatically generates a reset on the Cisco 7600 SSC-400. See Usage Guidelines below for details.

hw-module slot *slot* **subslot** *subslot* **only**

Syntax Description

slot	Chassis slot number where the Cisco 7600 SSC-400 is located. Refer to the appropriate hardware manual for slot information. For SIPs and SSCs, refer to the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide.
subslot	Secondary slot number on the SSC where the IPSec VPN SPA is installed.

Command Default

No default behavior or values.

Command Modes

Global configuration mode

Command History

Release	Modification
12.2(18)SXF2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2SXI	This command was deleted.

Usage Guidelines

Follow these guidelines and restrictions when configuring a Cisco 7600 SSC-400 and IPSec VPN SPAs using the **hw-moduleslotsubslotonly**command:

- This command is useful when supporting IP multicast over GRE on the IPSec VPN SPA.
- When this command is executed, it automatically takes a reset action on the Cisco 7600 SSC-400 and issues the following prompt to the console:

```
Module n will be reset? Confirm [n]:
```

The prompt will default to "N" (no). You must type "Y" (yes) to activate the reset action.

- When in this mode, if you manually plug in a second SPA, or if you attempt to reset the SPA (by entering a **nohw-modulesubslotshutdown** command, for example), a message is displayed on the router console which refers you to the customer documentation.

Examples

The following example allocates full buffers to the SPA that is installed in subslot 0 of the SIP located in slot 1 of the router and takes a reset action of the Cisco 7600 SSC-400.

```
Router(config)# hw-module slot 4 subslot 1 only
Module 4 will be reset? Confirm [no]: y
```

Note that the prompt will default to "N" (no). You must type "Y" (yes) to activate the reset action.

Related Commands

Command	Description
ip multicast-routing	Enables IP multicast routing.
ip pim	Enables Protocol Independent Multicast (PIM) on an interface.

hw-module standby

To reset the standby Route Processor (RP), use the **hw-modulestandby**command in privileged EXEC mode.

hw-module standby {**reset** | **reload**}

Syntax Description

reset	Resets the redundant RP.
reload	Reloads the redundant RP.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EX2	This command was introduced.
12.2(18)S	This command was introduced on Cisco 7304 routers running Cisco IOS Release 12.2(18)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to reset or reload the standby RP. Use the **reload** keyword to cause the standby RP to reload with an upgraded image. Use this option when the standby RP is operating normally. Use the **reset**keyword for a hard reset of the standby RP. Use this option if the standby RP is experiencing problems and does not respond to the **reload** option.

Examples

The following example shows how to reset the standby RP (NSE-100):

```
Router# hw-module standby reset
Proceed with reset of standby NSE? [confirm]y
```

The following example shows an attempt to reset a standby RP, which is down or experiencing some other problem such as being hung.

```
Router# hw-module standby reload
Proceed with reload of standby NSE? [confirm]y
%Standby RP is not up
```

If there is a failure to reset a standby RP because it is in some fault condition, try performing a reload of the RP.

The following example shows how to reload the standby RP:

```
Router# hw-module standby reload
Proceed with reload of standby NSE? [confirm]y
```

Related Commands

Command	Description
debug redundancy	Enables RP redundancy debugging.
redundancy force-switchover	Forces the standby RP to assume the role of the active RP.
show c7300	Displays the types of cards (RP and line cards) installed in a Cisco 7304 router.
show redundancy	Displays redundancy information for the active and standby RPs.

hw-module subslot

To restart, stop, or start a shared port adapter (SPA) and its interfaces, use the **hw-modulesubslot**command in privileged EXEC mode.

hw-module subslot *slot/subslot* {**reload** [**force**] | **start** | **stop** [**force**]}

For ASR 900 Series Routers, **hw-module** *slot* / *subslot* [**default** | **ether-mode 1G** | **ether-mode 10G**]

Syntax Description

slot	Physical slot number of the interface
subslot	Subslot of the interface
default	Default of all the interfaces of the interface module
ether-mode 1G	Mode of the ethernet imterface module
ether-mode 10G	Mode of the ethernet imterface module

Command Default

The SPA and its interfaces are not started.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(25)S3	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE on the Cisco 7600 series router and Catalyst 6500 series switch.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.4	This commad was modified. The **force** keyword was added. This command was integrated into Cisco IOS XE Release 2.4.
Cisco IOS XE 16.5.1 Everest	The keyword **ether-mode 1G** was introduced.

Usage Guidelines

The **hw-modulesubslot** command stops and starts power to the SPA. This command is useful when you want to restart all interfaces on a SPA. When the **stop** and **reload** keywords are used, you get a prompt to confirm. Enter “y” or use the return key to confirm. Power to the SPA is now stopped or reloaded. If you use the **force** keyword along with the **reload** keyword, you can proceed further without getting any prompt for confirmation. The Excalibur and Ethernet Services cards do not have the **reload** option.

The command is recommended to restart a SPA under the following conditions:

- To restart a SPA after it has been powered off because of a failure.
- To recover from corrupted messaging between the Route Processor (RP) and the SIP.

Examples

The following command power cycles the SPA in subslot 1 of the SIP installed in chassis slot 1:

```
Router# hw-module subslot 1/1 reload
Proceed with reload of module? [confirm]
```

Related Commands

Command	Description
show hw-module subslot oir	Displays the operational status of a SPA.

hw-module subslot (4400)

To restart, stop, or start a module and its interfaces, use the **hw-modulesubslot** command in privileged EXEC mode.

hw-module subslot *slot/subslot* {**reload** | **start** | **stop** }

Syntax Description

reload	Restarts the target subslot.
slot	Specifies the chassis slot number where the module is installed. Refer to the hardware installationg guide for more information on slots. For module and interfaces, refer to the module-specific hardware installation guide.
start	Activates the specified module.
stop	Stops the specified module.
/ *subslot*	Specifies the subslot number of the chassis where the module is installed. Refer to the hardware installation guide for subslot information.

Command Default

The modules and its interfaces are not activated.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced.

Usage Guidelines

The **hw-module subslot** command allows you to stop and start the power supply to a supported cisco services or network interface module (NIM) on a Cisco 4400 Series Integrated Services Router (ISR). This functionality is also referred as the online insertion and removal (OIR) and it is useful when you want to remove a module from one of the subslots while another active module remains installed on your router.

Note If you are not planning to immediately replace a module, ensure that you install a blank filter plate in the subslot.

The **stop** option allows you to gracefully deactivate a module and the module is rebooted when the **start** command is executed. The **reload** option will stop or deactivate a specified module and restart it.

Examples

The following command activates a module in subslot 1:

```
Router# hw-module subslot 1/1 start
```

Related Commands

Command	Description
show hw-module subslot oir	Displays the operational status of a module.

hw-module subslot ethernet vlan unlimited

To remove the restriction of a maximum of 8100 IEEE 802.1Q VLANs per Ethernet shared port adapter (SPA), use the **hw-modulesubslotethernetvlanunlimited** command in global configuration mode. To disable and return to a maximum limit of 8100 VLANs per SPA, use the **no** form of this command.

hw-module subslot *slot/subslot* **ethernet vlan unlimited**
no hw-module subslot *slot/subslot* **ethernet vlan unlimited**

Syntax Description

slot /	Specifies the chassis slot number where the SIP is installed.
subslot	Specifies the slot of the SIP where the SPA is installed.

Command Default

There is no default behavior or values. When this command is not configured, up to 8100 dot1q VLANs per Ethernet SPA are supported.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.5	This command was introduced.

Usage Guidelines

For any Ethernet SPA on the Cisco ASR 1000 Series aggregation services routers, the maximum number of IEEE 802.1Q VLANs that can be configured per port is 4094. The default total maximum number of VLANs per SPA is 8100.

The limit on this total maximum number of VLANs per SPA (which means, the default of 8100 VLANs) can be removed using the **hw-modulesubslotethernetvlanunlimited** command. However, the limit on the maximum number of VLANs per Ethernet port or interface (i.e. 4094) still applies. Therefore, the new maximum number of supported VLANs per SPA varies by the number of ports on the SPA multiplied by 4094. On the 5-Port Gigabit Ethernet SPA, you can configure up to 20,470 dot1q (or unambiguous QinQ) VLANs. On an 8-Port Gigabit Ethernet SPA, you can configure up to 32752 dot1q (or unambiguous QinQ) VLANs.

When the **hw-modulesubslotethernetvlanunlimited** command is configured, VLAN filtering, accounting, and classification are no longer performed by the Ethernet SPA and all 802.1Q frames and QinQ frames are processed by the Quantum Flow Processor (QFP) on the Cisco ASR1000 Series Router. Sending all of the dot1q VLAN frames to the QFP (without filtering) may reduce the QFP packet switching performance.

The default classification of CoS bits 6-7 as high priority is still supported. However, other user-defined CoS values for high and low priority classification using the **plimqosinputmapcosqueue** command are not supported when this command is in use.

Examples

The following example enables support for maximum per-port dot1q VLAN configuration for the SPA located in the first subslot (0) of the SIP located in slot 1 of the Cisco ASR1000 Series Router:

```
Router(config)# hw-module subslot 1/0 ethernet vlan unlimited
```

Related Commands

Command	Description
show interfaces	Displays statistics for all interfaces configured on the router.

hw-module subslot (LAN WAN)

To configure the Cisco 1-Port 10 Gigabit Ethernet LAN/WAN-PHY Shared Port Adapter to run in either the LAN mode or WAN mode, use the **hw-modulesubslotslot/subslotenable{LAN|WAN}**commandin Global configuration mode.

hw-module subslot *slot/subslot* **enable** {**LAN** | **WAN**}

Syntax Description

slot/subslot	The slot and subslot number in which the Cisco 1-Port 10 Gigabit Ethernet LAN/WAN-PHY Shared Port Adapter has been installed.
enable	Enables the specified LAN or WAN operational mode on the SPA.
LAN	Specifies the LAN mode of operation for theCisco 1-Port 10 Gigabit Ethernet LAN/WAN-PHY Shared Port Adapter.
WAN	Specifies the WAN mode of operation for the Cisco 1-Port 10 Gigabit Ethernet LAN/WAN-PHY Shared Port Adapter.

Command Default

By default, the Cisco 1-Port 10 Gigabit Ethernet LAN/WAN-PHY Shared Port Adapter operates in the WAN mode when the SPA boots-up.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.3.0S	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines

By default, the Cisco 1-Port 10 Gigabit Ethernet LAN/WAN-PHY Shared Port Adapter initializes in the WAN mode. The Cisco 1-Port 10 Gigabit Ethernet LAN/WAN-PHY Shared Port Adapter can operate in either the LAN mode or the WAN mode. To change the LAN mode or WAN mode, execute the **hw-modulesubslot***slot/subslot***enable** {**LAN** | **WAN**} command from the Global configuration mode.

Examples

The following example shows how to enable the LAN mode on a Cisco 1-Port 10 Gigabit Ethernet LAN/WAN-PHY Shared Port Adapter:

```
Router# config
Router(config)# hw-module subslot 2/1 enable LAN
```

The following example shows how to enable the WAN mode on a Cisco 1-Port 10 Gigabit Ethernet LAN/WAN-PHY Shared Port Adapter:

```
Router# config
Router(config)# hw-module subslot 2/1 enable WAN
```

Tip

If the Cisco 1-Port 10 Gigabit Ethernet LAN/WAN-PHY Shared Port Adapter is working in LAN mode, you can change the mode to WAN by either using the **hw-modulesusblot***slot/subslot***enableWAN** command.

Related Commands

Command	Description
show controllers wanphy	Displays the SPA mode (LAN mode or WAN mode), alarms, and the J1 byte string value.

hw-module subslot service-engine session

To open a console session to access the Cisco WebEx Node SPA console, use the **hw-modulesubslotservice-enginesession**command in privileged EXEC mode.

hw-module subslot *slot/subslot* **service-engine session**

Syntax Description

slot	Specifies the chassis slot number for the Cisco ASR 1000 Series Router SIP.
/ *subslot*	Specifies the secondary subslot number on a Cisco ASR 1000 Series Router SIP where a SPA is installed.

Command Default

No command default.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
IOS XE Release 2.4	This command was introduced.

Usage Guidelines

To open a console session on a Cisco WebEx Node SPA, the SPA must first be configured with a minimum of the following commands:

- **ip address**
- **service-engine ip address**
- **service-engine default-gateway**

The **service-engineipaddress** command must be configured before the **service-enginedefault-gateway** command.

Examples

The following example shows how to access the console for a WebEx Node SPA located in slot 1/0, and the change to the SPA console prompt (service-spa is the default hostname) when complete:

```
Router# hw-module subslot 1/0 service-engine session
MontaVista(R) Linux(R) Carrier Grade Edition 5.0 (custom)
Linux/mips64 2.6.21_mvlcge500-octeon-mips64_octeon_v2_be
        Vegas Shell  --  CGE 5.0 Version
        Copyright (c) 1985-2008 by Cisco Systems, Inc.
        All rights reserved.
service-spa#
```

Related Commands

Command	Description
service-engine default-gateway	Defines a default gateway router IP address for the Cisco WebEx Node SPA.

Command	Description
service-engine ip address	Selects and configures the internal interface for management traffic on a Cisco WebEx Node SPA.

hw-module subslot session

To start or close a Cisco Integrated Management Controller (CIMC) session or host server module session, use the **hw-module subslot session** command in privileged EXEC mode.

hw-module subslot *slot/subslot* **session** {**imc** | **server**}

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the NIM E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot number is 0.
imc	Starts a session with CIMC.
server	Starts a session with the host server module.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced on the Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Router (ISR).
Cisco IOS XE Release 3.15S	This command was supported on an additional platform: the NIM E-Series Network Compute Engine (NIM E-Series NCE) installed in a Cisco ISR 4000 series.

Usage Guidelines

Only one active session is allowed on the CIMC or server module at any time.

Examples

The following example shows how to start a CIMC session in an E-Series Server installed in a Cisco ISR 4000 series:

```
Router# hardware-module subslot 1/0 session imc
```

The following example shows how to start a server module session in an E-Series Server installed in a Cisco ISR 4000 series:

```
Router# hardware-module subslot 1/0 session server
```

hw-module subslot shutdown

To disable a shared port adapter (SPA) with or without power, and save the configuration to the configuration file, use the **hw-modulesubslotshutdown**command in global configuration mode. To re-enable the SPA, use the **no** form of this command.

hw-module subslot *slot/subslot* **shutdown** [{**powered** | **unpowered**}]
no hw-module subslot *slot/subslot* **shutdown** [{**powered** | **unpowered**}]

Syntax Description

slot	Chassis slot number. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide.
/ *subslot*	Secondary slot number on a SPA interface processor (SIP) where a SPA is installed. Refer to the platform-specific SPA hardware installation guide and the corresponding "Specifying the Interface Address on a SPA" topic in the platform-specific SPA software configuration guide for subslot information.
powered	(Optional) Shuts down the SPA and all of its interfaces, and leaves them in an administratively down state with power enabled. This is the default state.
unpowered	(Optional) Shuts down the SPA and all of its interfaces, and leaves them in an administratively down state wihout power.

Command Default

If this command is not used, **nohw-modulesubslotshutdown** is the default behavior. When **nohw-modulesubslot** is configured, the SPA will be powered for normal operation.

If the **hw-modulesubslotshutdown** command is entered but neither **powered** or **unpowered** are specified in the CLI, **powered** is the default behavior.

Command Modes

Global configuration

Command History

Release	Modification
12.2(25)S3	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

When you shut down a SPA using this command, you can choose to put it into one of two states:

- Powered state--(Default) Shuts down the SPA, but the SPA remains powered on. Use this option when you plan to leave the SPA physically installed and cabled in the SPA. You might choose to do this if you want to install a SPA and configure it, but do not want it online or to start communicating with the remote end of the connection.

- Unpowered state--Shuts down the SPA and removes power from the SPA. Use this option when you plan to remove the SPA from the chassis.

This command is useful when a user wants all the interfaces on a SPA disabled but does not or cannot remove the SPA. Unlike the **hw-modulesubslotstop** EXEC command on the Cisco 7304 router, this command is saved in the configuration file and will keep the SPA disabled when other router events (such as a router reload or OIR) attempt to restart the SPA. All other settings and configurations of the SPA will be maintained even if the SPA itself is shutdown using this command.

As a general rule, you do not need to shut down a SPA if you are removing it and replacing it with the same exact model of SPA in an online insertion and removal (OIR) operation. However, you should shut down a SPA whenever you are replacing a SPA with a different model of SPA.

When you shut down a SPA using the **hw-modulesubslotshutdown**command, it remains shutdown even if you reset the SPA or install a new SPA in that subslot. To begin using the card again, you must manually re-enable the card using the **nohw-modulesubslotshutdown**command.

Note This is a global configuration command, not an EXEC command. On the Cisco 7304 router, another **hw-modulesubslot** command is also available in EXEC mode, but that command is used for different purposes. An important distinction between this command and the **hw-modulesubslot** command in EXEC mode on the Cisco 7304 router is that this command is saved in the configuration.

Examples

The following example shows how to disable the SPA in subslot 4/1 while leaving the SPA in the SPA chassis. This command will be saved to the configuration file and no actions, outside of changing this configuration, will re-enable the SPA:

```
Router(config)# hw-module subslot 4/1 shutdown unpowered
```

The following example shows how to configure the SPA to resume normal operation after the unpowered option has been used to disable the SPA:

```
Router(config)# hw-module subslot 4/1 shutdown powered
```

No messages are provided on the console when you shut down or re-enable a SPA.

Related Commands

Command	Description
show hw-module subslot oir	Displays the operational status of a SPA.
hw-module slot [1]	Deactivates or reactivates a carrier card that is installed in a router slot. This command is entered in EXEC mode and is not saved to the configuration file.

1 Refer to the Cisco 7300 Series Platform-Specific Commands publication.

hw-module subslot shutdown (4400)

To disable a module with or without power, and save the configuration to the configuration file, use the **hw-module subslot shutdown** command in global configuration mode. To re-activate the module, use the **no** form of this command.

hw-module subslot *slot /subslot* **shutdown** [{**powered** | **unpowered**}]
no hw-module subslot *slot /subslot* **shutdown** [{ **powered** | **unpowered** }]

Syntax Description

slot	Specifies the chassis slot number where the module installed. Refer to the hardware installation guide for more information on slots. For information on modules and interfaces, refer to the module specific hardware installation guide.
/ *subslot*	Specifies the subslot number of the chassis where the module is installed. Refer to the hardware installation guide for subslot information.
powered	(Optional) Shuts down the module and all of its interfaces, and leaves them in an administratively down state with power enabled. This is the default state.
unpowered	(Optional) Shuts down the module and all of its interfaces, and leaves them in an administratively down state without power.

Command Default

If this command is not used, **no hw-module subslot shutdown** is the default behavior. When **no hw-module subslot** is configured, the module is powered on for normal operation.

If the **hw-module subslot shutdown** command is entered but neither **powered** or **unpowered** are specified in the CLI, **powered** is the default behavior.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced.

Usage Guidelines

When you shut down a Cisco Services or Network Interface Module (NIM) using this command, you can choose to put it into one of two states:

- Powered state--(Default) Shuts down the module, but the router remains powered on. Use this option when you plan to leave the module physically installed and cabled into the router. You might choose to do this if you want to install a module and configure it, but do not want it online or to start communicating with the remote end of the connection.
- Unpowered state--Shuts down the module and removes power from the module. Use this option when you plan to remove the module from the chassis.

If you choose to deactivate your module and its interfaces by executing the **hw-module subslot shutdown** command in global configuration mode, you are able to change the configuration in such a way that no matter how many times the router is rebooted, the module does not boot. This command is useful when you need to shut down a module located in a remote location and ensure that it does not boot automatically when the router is rebooted. To begin using the interface again, you must manually re-enable the module using the **no hw-module subslot shutdown** command.

Examples

The following example shows how to disable the module in subslot 0/2 without removing the module from the router :

```
Router(config)# hw-module subslot 0/2 shutdown unpowered
```

The following example shows how to configure a module to resume normal operation after the unpowered option has been used to disable the module:

```
Router(config)# hw-module subslot 0/2 shutdown powered
```

Related Commands

Command	Description
show hw-module subslot oir	Displays the operational status of a module.
hw-module subslot	Deactivates or reactivates a module in a router slot. This command is entered in EXEC mode and is not saved to the configuration file.

I through K

id aa-group

To configure the asynchronous acknowledgement group ID, use the **idaa-group**command in satellite initial configuration mode. To remove the ID configuration, use the **no** form of this command.

id aa-group *number*
no id aa-group

Syntax Description

aa-group	Asynchronous acknowledgement group ID.
number	ID number in the range from 256 to 511.

Command Default

No default behavior or values

Command Modes

Satellite initial configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

This command is typically used by an installation technician. Do not use this command unless your satellite service provider instructs you to perform the satellite initial configuration and provides all necessary parameter values.

Examples

The following example shows how to configure the asynchronous acknowledgement group identification number:

```
Router(sat-init-config)# id aa-group 336
```

id software group

To configure the operational software group identification number, use the **idsoftwaregroup**command in satellite initial configuration mode. To remove the ID configuration, use the **no** form of this command.

id software group *number*
no id software group

Syntax Description

number	ID number in the range from 512 to 767.

Command Default

No default behavior or values

Command Modes

Satellite initial configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

This command is typically used by an installation technician. Do not use this command unless your satellite service provider instructs you to perform the satellite initial configuration and provides all necessary parameter values.

Examples

The following example shows how to configure the operational software group identification number:

```
Router(sat-init-config)# id software group 598
```

id vsat

To configure the component physical address (CPA), use the **idvsat**command in satellite initial configuration mode. To remove the CPA configuration, use the **no** form of this command.

id vsat *number*
no id vsat *number*

Syntax Description

number	CPA number in the range from 1280 to 32766.

Command Default

No default behavior or values

Command Modes

Satellite initial configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(22)T	The CPA number range was increased to 32766.

Usage Guidelines

The CPA uniquely identifies the VSAT endpoint in the satellite network.

Note This command is typically used by an installation technician. Do not use this command unless your satellite service provider instructs you to perform the satellite initial configuration and provides all necessary parameter values.

Examples

The following example shows how to configure the CPA number:

```
Router(sat-init-config)# id vsat 1284
```

idle-pattern

To define the idle pattern that a circuit emulation (CEM) channel transmits when the channel experiences an underrun condition or to replace any missing packets, use the **idle-pattern**command in CEM configuration mode. To stop sending idle pattern data, use the **no** form of this command.

idle-pattern {*pattern* | *length* *pattern1* [*pattern2*]}
no idle-pattern

Syntax Description

pattern	An 8-bit hexadecimal number. T1 and E1 channels require only this argument.
length	Length, in bits, of the pattern. Serial cards require that you enter a value for *length* .
pattern1	Specifies (in hex notation) up to 32 bits of the least significant bits of the idle data pattern. Default is 0xFF.
pattern2	(Optional) Specifies (in hex notation) the most significant bits of the idle data pattern. If the *length* argument is 32 bits or less, this argument is not permitted.

Command Default

For T1 or E1 channels, the default idle pattern is 0xFF. For serial channels, the default idle pattern is 0xFF and 8 bits in length.

Command Modes

CEM configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
XE 3.18SP	This command is integrated in Cisco NCS 4200 Series.

Usage Guidelines

Idle pattern data is always sent in multiples of one entire packet payload. If a single packet is missing from the arriving data stream it is replaced by an idle packet of the same payload size and composed of repetitions of the specified idle pattern. If the CEM channel outbound (egress) buffer experiences an underrun condition, identical idle packets are transmitted until the dejitter buffer is filled to at least half its total depth.

Examples

The following example shows how to configure a 32-bit idle pattern for a serial CEM channel.

```
Router(config-cem)# idle-pattern 32 0x12345678
```

Related Commands

Command	Description
cem	Enters circuit emulation configuration mode.
clear cem	Clears CEM channel statistics.
show cem	Displays CEM channel statistics.

ids-service-module monitoring

To enable Intrusion Detection System (IDS) monitoring on a specified interface, use the **ids-service-modulemonitoring** command in interface configuration mode. To perform IDS monitoring, the routing device must have a Cisco IDS network module installed. To disable IDS monitoring, use the **no** form of this command.

ids-service-module monitoring
no ids-service-module monitoring

Syntax Description

This command has no arguments or keywords.

Command Default

IDS monitoring is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

Use the **ids-service-modulemonitoring** command to enable IDS monitoring on a specified interface or subinterface. Both inbound and outbound packets on the specified interface are forwarded for monitoring.

The Cisco IDS network module is also referred to as the NM-CIDS.

Examples

The following example shows how to configure Fast Ethernet interface 0/0 to copy network traffic to the Cisco IDS network module and enable IDS monitoring:

```
Router(config)# interface FastEthernet0/0
Router(config-if)# ids-service-module monitoring
```

Related Commands

Command	Description
service-module ids-sensor	Reboots, resets, enables console access to, shuts down, and monitors the status of the Cisco IDS network module.

if-mgr delete

To delete the unused interface identification numbers (ifIndex) from the system interface, use the **if-mgrdelete** command in privileged EXEC mode.

if-mgr delete {**ifindex-pool** *initial-ifindex number-of-ifindexes* | **interfaceType** *interface-name*}

Syntax Description

ifindex-pool	Specifies the ifIndex pool to delete.
initial-ifindex	Initial ifIndex value in the ifIndex pool. The range is from 1 to 3200.
number-of-ifindexes	The number of ifIndexes to be deleted. The range is from 1 to 3200.
interfaceType	Specifies the type of interface to which the ifIndex value is assigned.
interface-name	Name of the interface to which the ifIndex is assigned.

Command Default

The ifIndexes assigned for the specified system interface are deleted.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2 SXH	This command was introduced.

Usage Guidelines

The ifIndex is a unique identification value associated with a physical or logical interface.

While specifying the ifIndex to be deleted, also provide the interface description (ifDescr) and the ifindex value assigned to that interface.

Examples

The following example shows how to delete the pool of unused ifIndexes:

```
Router# if-mgr delete ifindex-pool 2 5
```

Related Commands

Command	Description
show snmp mib ifmib ifindex	Displays all SNMP ifIndex identification numbers for all system interfaces.

ignore (interface)

To configure the serial interface to ignore the specified serial signals as the line up/down indicator, use the **ignore**command in interface configuration mode. To restore the default, use the **no** form of this command.

DCE Asynchronous Mode
ignore [{**dtr** | **rts**}]
no ignore [{**dtr** | **rts**}]

DCE Synchronous Mode
ignore [{**dtr** | **local-loopback** | **rts**}]
no ignore [{**dtr** | **local-loopback** | **rts**}]

DTE Asynchronous Mode
ignore [{**cts** | **dsr**}]
no ignore [{**cts** | **dsr**}]

DTE Synchronous Mode
ignore [{**cts** | **dcd** | **dsr**}]
no ignore [{**cts** | **dcd** | **dsr**}]

Syntax Description

dtr	Specifies that the DCE ignores the Data Terminal Ready (DTR) signal.
rts	Specifies that the DCE ignores the Request To Send (RTS) signal.
local-loopback	Specifies that the DCE ignores the local loopback signal.
cts	Specifies that the DTE ignores the Clear To Send (CTS) signal.
dsr	Specifies that the DTE ignores the Data Set Ready (DSR) signal.
dcd	Specifies that the DTE ignores the Data Carrier Detect (DCD) signal.

Command Default

The **no** form of this command is the default. The serial interface monitors the serial signal as the line up/down indicator.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(15)ZJ	This command was introduced on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, and Cisco 3745 routers.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.

Usage Guidelines

Serial Interfaces in DTE Mode

When the serial interface is operating in DTE mode, it monitors the DCD signal as the line up/down indicator. By default, the attached DCE device sends the DCD signal. When the DTE interface detects the DCD signal, it changes the state of the interface to up.

SDLC Multidrop Environments

In some configurations, such as a Synchronous Data Link Control (SDLC) multidrop environment, the DCE device sends the DSR signal instead of the DCD signal, which prevents the interface from coming up. Use this command to tell the interface to monitor the DSR signal instead of the DCD signal as the line up/down indicator.

Examples

The following example shows how to configure serial interface 0 to ignore the DCD signal as the line up/down indicator:

```
Router(config)# interface serial 0
Router(config-if)# ignore dcd
```

Related Commands

Command	Description
debug serial lead-transition	Activates the leads status transition debug capability for all capable ports.
show interfaces serial	Displays information about a serial interface.

ignore-dcd

To configure the serial interface to monitor the Data Set Ready (DSR) signal instead of the Data Carrier Detect (DCD) signal as the line up/down indicator, use the **ignore-dcd** command in interface configuration mode. To restore the default, use the **no** form of this command.

ignore-dcd
no ignore-dcd

Syntax Description

This command has no arguments or keywords.

Command Default

The serial interface, operating in DTE mode, monitors the DCD signal as the line up/down indicator.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command applies to Quad Serial NIM interfaces on the Cisco 4000 series routers and Hitachi-based serial interfaces on the Cisco 2500 and Cisco 3000 series routers.

Serial Interfaces in DTE Mode

When the serial interface is operating in DTE mode, it monitors the DCD signal as the line up/down indicator. By default, the attached DCE device sends the DCD signal. When the DTE interface detects the DCD signal, it changes the state of the interface to up.

SDLC Multidrop Environments

In some configurations, such as an Synchronous Data Link Control (SDLC) multidrop environment, the DCE device sends the DSR signal instead of the DCD signal, which prevents the interface from coming up. Use this command to tell the interface to monitor the DSR signal instead of the DCD signal as the line up/down indicator.

Examples

The following example shows how to configure serial interface 0 to monitor the DSR signal as the line up/down indicator:

```
Router(config)# interface serial 0
Router(config-if)# ignore-dcd
```

ignore-error-duration

To ignore initial train-up errors when the DSL controller is connected to DSLAMs with chipsets other than Globespan, use the**ignore-error-duration** command in controller configuration mode. To set the error duration to the default of 0 seconds, use the **no** form of the command.

ignore-error-duration *seconds*

Syntax Description

seconds	Sets the time in seconds for which errors will be ignored during training of the line. Range is from 15 to 30 seconds.

Command Default

0 seconds

Command Modes

Controller configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced on Cisco 2600 series and Cisco 3700 series routers.
12.3(4)XG	This command was integrated into the Cisco IOS Release 12.3(4)XG on the Cisco 1700 series routers.
12.3(7)T	This command was implemented on Cisco 2600 series, Cisco 3631, and Cisco 3700 series routers.
12.3(11)T	This command was implemented on Cisco 2800 and Cisco 3800 series routers.
12.3(14)T	This command was implemented on Cisco 1800 series routers.

Usage Guidelines

This command is used to ignore initial train-up errors when connected to DSLAMs with chipsets other than Globespan. Use the time period of 15 to 30 seconds to allow the line to train without being affected by errors that result because of the line training.

Examples

The following example sets the time during which errors will be ignored to 15 seconds:

```
Router(config)# controller dsl
4/0
Router(config-controller)# ignore-error-duration
15
```

Related Commands

Command	Description
controller dsl	Configures the DSL controller.

ignore-hw local-loopback

To disable the monitoring of the (local-loopback) LL pin when in DCE mode, use the **ingnore-hwlocal-loopback** command in interface configuration mode. To enable the monitoring of the LL pin, use the **no** form of this command.

ignore-hw local-loopback
no ignore-hw local-loopback

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command if your system is experiencing spurious modem interrupts that momentarily cause the interface to enter loopback mode. The end result of this behavior is the loss of Synchronous Data Link Control (SDLC) Logical Link Control (SDLLC) sessions.

Note This command works only with the low-speed serial interfaces.

Examples

The following example shows how to disable the monitoring of the LL pin when in DCE mode:

```
Router(config)# interface serial 2
Router(config-if)# ignore-hw local-loopback
```

imc access-port

To configure Cisco Integrated Management Controller (CIMC) access through the server module's dedicated, management, or host ports, use the **imc access-port** command in interface configuration mode or UCSE configuration mode.

Cisco UCS E-Series Server Installed in Cisco 2900 and 3900 ISR G2 and the Cisco ISR 4451-X

imc access-port {**dedicated** | **shared-lom** [{**GE1** | **GE2** | **GE3** | **console** | **failover** [*option*]}]}

no imc access-port {**dedicated** | **shared-lom** [{**GE1** | **GE2** | **GE3** | **console** | **failover** [*option*]}]}

Cisco UCS E-Series Server Installed in the Cisco ISR 4451-X—Applicable Only with Cisco IOS XE Release 3.9S

imc access-port {**MGMT** | [{**GE0** | **GE1** | **GE2** | **GE3**[*failover-option*]}]}

no imc access-port {**MGMT** | [{**GE0** | **GE1** | **GE2** | **GE3**[*failover-option*]}]}

Syntax Description

Table 18: Cisco UCS E-Series Server Installed in Cisco 2900 and 3900 ISR G2 and the Cisco ISR 4451-X

dedicated	Configures CIMC access using the IMC dedicated port.
shared-lom	Configures CIMC access using one of the following host ports: • **GE1** • **GE2** • **GE3** • **console** • **failover** **Note** If you enter **failover**, you must also enter one additional parameter: • **GE1 GE1** [**GE2**] | [**GE3**] [**GE2 GE3**] • **GE2 GE2 GE3**

Table 19: Cisco UCS E-Series Server Installed in the Cisco ISR 4451-X—Applicable Only with Cisco IOS XE Release 3.9S

MGMT	Configures CIMC access using the Cisco UCS E-Series Server's management port.

GE0, **GE1**, **GE2**, **GE3**	(Optional) Configures CIMC access using one of the following NIC interfaces:
	• **GE0**—Cisco UCS E-Series Server's internal NIC interface connecting to the router's UCSE *slot*/**0**/**0** interface.
	• **GE1**—Cisco UCS E-Series Server's internal NIC interface connecting to the router's UCSE *slot*/**0**/**1** interface.
	• **GE2**—Cisco UCS E-Series Server's external NIC interface.
	• **GE3**—Cisco UCS E-Series Server's external NIC interface. Applicable to double-wide Cisco UCS E-Series Servers.
	• *failover-option*—To configure failover, enter one additional parameter:
	  • **GE2 backplane**—Applicable to single-wide and double-wide Cisco UCS E-Series Servers.
	  • **GE3 backplane**—Applicable to double-wide Cisco UCS E-Series Servers.
	  • **GE2 GE3**—Applicable to double-wide Cisco UCS E-Series Servers.
	  • **GE3 GE2**—Applicable to double-wide Cisco UCS E-Series Servers.
	  • **GE2 GE3 backplane**—Applicable to double-wide Cisco UCS E-Series Servers.
	  • **GE3 GE2 backplane**—Applicable to double-wide Cisco UCS E-Series Servers.

Command Modes

Interface configuration (config-if) for a Cisco UCS E-Series Server installed in Cisco 2900 and 3900 ISR G2.

UCSE configuration (config-ucse) for a Cisco UCS E-Series Server installed in the Cisco ISR 4451-X.

Command History

Release	Modification
Cisco IOS Release 15.2(4)M	This command was introduced on the Cisco UCS E-Series Servers installed in Cisco 2900 and 3900 Series Integrated Services Routers (ISR G2).
Cisco IOS XE Release 3.9S	This command was implemented on Cisco UCS E-Series Servers installed in the Cisco 4451-X Integrated Services Router (Cisco ISR 4451-X).
Cisco IOS XE Release 3.10S	This command was modified so that all platforms—Cisco 2900 and 3900 ISR G2 and the Cisco ISR 4451-X—use the same command.

Usage Guidelines

If the Cisco UCS E-Series Server is installed in Cisco 2900 and 3900 ISR G2, use the **imc access-port** command in interface configuration mode:

```
Router(config)# interface ucse 2/0
Router(config-if)#
```

If the Cisco UCS E-Series Server is installed in Cisco ISR 4451-X, use the **imc access port** command in UCSE configuration mode:

```
Router(config)# ucse subslot 1/0
Router(config-ucse)#
```

Examples

The following example shows how to configure CIMC access using the dedicated port:

```
Router# configure terminal
Router(config)# interface ucse 2/0
Router(config-if)# imc ip address 10.0.0.2 255.0.0.0 default-gateway 10.0.0.1
Router(config-if)# imc access-port dedicated
Router(config-if)# no shut
Router(config-if)# end
```

Cisco UCS E-Series Server Installed in the Cisco ISR 4451-X—Applicable Only with Cisco IOS XE Release 3.9S

The following example shows how to configure CIMC access using the MGMT port:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ucse subslot 1/0
Router(config-ucse)# imc access-port mgmt
Router(config-ucse)#
 IMC ACK: Access ports received: MGMT

 IMC ACK: UCSE access port operation successful.
```

imc config file

To store the name of a CIMC configuration file in the running configuration, use the **imc config file** command from interface configuration mode .

imc config file *file_name*
no imc config file *file_name*

Syntax Description

file_name	The name of the CIMC configuration file that you want to store.

Command Modes

Interface configuration mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

Use this command from interface configuration mode:

```
Router(config)# interface ucse slot/port
```

Examples

The following example shows how to store a configuration CIMC file to the running configuration. Note that there is no output after you issue the command:

```
Router(config)# interface ucse 2/0
Router(config-if)# imc config file flash0:my-imc-config
```

imc dns

To configure a domain name system (DNS) server for CIMC, use the **imc dns** command from interface configuration mode.

imc dns
no imc dns

Syntax Description

This command has no arguments.

Command Modes

Interface configuration mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

Use this command from interface configuration mode:

```
Router(config)# interface ucse slot/port
```

Examples

The following example shows how to configure the DNS server for CIMC:

```
Router(config)# interface ucse 2/0
Router(config-if)# imc dns
```

imc ip address default-gateway

To configure a static IP address for CIMC and the IP address of the default gateway router that CIMC must use, use the **imc ip address default-gateway** command in interface configuration mode. To remove the static IP address, use the **no** form of this command.

imc ip address *ip-address subnet-mask* **default-gateway** *gateway-address*
no imc ip address *ip-address subnet-mask* **default-gateway** *gateway-address*

Syntax Description

ip-address	IP address of CIMC.
subnet-mask	Subnet mask to append to the IP address; must be in the same subnet as the host router.
gateway-address	IP address of the default gateway router.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

If you do not enable DHCP, you must specify a static IP address and subnet mask.

Examples

The following example shows how to configure a static IP address for CIMC:

```
Router(config)# interface ucse 2/0
Router(config-if)# imc ip address 10.0.0.2 255.0.0.0 default-gateway 10.0.0.1
```

imc ip address dhcp

To configure a DHCP IP address for CIMC, use the **imc ip address dhcp** command in interface configuration mode. To remove the DHCP IP address, use the **no** form of the this command.

imc ip address dhcp
no imc ip address dhcp

Syntax Description

This command has no arguments or keywords.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.2(4)M	This command was introduced.

Examples

The following example shows how to configure a DHCP IP address for CIMC:

```
Router(config)# interface ucse 2/0
Router(config-if)# imc ip address dhcp
```

imc ip dhcp

To configure a DHCP IP address for the Cisco Integrated Management Controller (CIMC), use the **imc ip dhcp** command in UCSE configuration mode. To remove the DHCP IP address, use the **no** form of this command.

imc ip dhcp
no imc ip dhcp

Syntax Description

This command has no arguments or keywords.

Command Modes

UCSE configuration (config-ucse)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced on the Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Router (ISR).

Examples

The following example shows how to configure a dynamic IP address for CIMC:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ucse subslot 1/0
Router(config-ucse)# imc ip dhcp
Router(config-ucse)#
 IMC ACK: DHCP enable received for IMC.

 IMC ACK: UCSE setting DHCP enable for IMC successful.
```

imc remote-manager

To configure the IP address of the remote manager, use the **imc remote-manager** command from interface configuration mode .

imc remote-manager *ip_address*
no imc remote-manager

Syntax Description

ip_address	IP address of the remote manager.

Command Modes

Interface configuration mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

Use this command from interface configuration mode:

```
Router(config)# interface ucse slot/port
```

Examples

The following example shows how to configure the IP address of the remote manager:

```
Router(config)# interface ucse 2/0
Router(config-if)# imc remote-manager 10.0.0.0
```

imc vlan

To enter VLAN configuration mode for the specified VLAN number, use the **imc vlan** command in interface configuration mode. To remove the VLAN configuration, use the **no** form of this command.

imc vlan *vlan-number*
no imc vlan *vlan-number*

Syntax Description

vlan-number	IP address of the remote manager.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.2(4)M	This command was introduced.

Examples

The following example shows how to enter VLAN configuration mode in CIMC for a specified VLAN:

```
Router(config)# interface ucse 2/0
Router(config-if)# interface vlan 40
```

input

To enable Precision Time Protocol input clocking using a 1.544Mhz, 2.048Mhz, or 10Mhz timing interface or phase using the 1PPS or RS-422 interface, use the **input** command in global configuration mode. To disable PTP input, use the **no** form of this command.

input [**1pps**] *slot/bay*
no input [**1pps**] *slot/bay*

Syntax Description

1pps	Configures the device to receive 1 pulse per second (1PPS) time of day messages using the RS422 port or 1PPS port. You can select 1PPS with or without selecting a timing port.
slot	Slot of the 1PPS interface.
bay	Bay of the 1PPS interface.

Command Default

Precision Time Protocol input clocking is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Usage Guidelines

If you are using GPS to provide clock source to the device, configure this command in PTP master mode.

This command applies only to platforms that have a 1PPS port.

Examples

The following example shows how to configure PTP input clocking:

```
Device> enable
Device# configure terminal
Device(config)# ptp clock ordinary domain 0
Device(config-ptp-clk)# input 1pps 3/1
Device(config-ptp-clk)# clock-port masterport master
```

Related Commands

Command	Description
output	Enables output of time of day messages using the 1PPS interface.

interface

To configure an interface type and to enter interface configuration mode, use the **interface** command in the appropriate configuration mode.

Standard Syntax
interface *type* *number* [*name-tag*]

Module-Specific and Platform-Specific Syntax

Analysis Module Network Module
interface **analysis-module** *slot*/*unit*

Content Engine Network Module
interface **content-engine** *slot*/*unit*

Cisco 830 Series
interface *type* [*number*]

Cisco 2600 Series
interface *type* *slot*/{*port-adapter* | *port* **.** *subinterface-number*}

Cisco 2600 Series on Voice Interfaces
interface *type* *slot*/*voice-module-slot*/*voice-interface-slot*

Cisco 3600 Series
interface *type* *slot*/{*port* | *port* **.** *subinterface-number*}

Cisco 3600 Series on Voice Interfaces
interface *type* *slot*/*voice-module-slot*/*voice-interface-slot*

Cisco 4400 Series Integrated Services Router (ISR)
interface *type* *number*

Cisco 7100 Series
interface *type* *slot*/{*port-adapter* | *port* **.** *subinterface-number*}

Cisco 7200 Series and Cisco 7500 Series with a Packet over SONET Interface Processor
interface *type* *slot*/*port*

Cisco 7200 VXR Router Used as a Router Shelf in a Cisco AS5800 Universal Access Server
interface *type* *router-shelf*/*slot*/*port*

Cisco 7500 Series with Channelized T1 or E1
interface **serial** *slot*/*port* **:** *channel-group*

Cisco 7500 Series with Ports on VIP Cards
interface *type* *slot*/*port-adapter*/*port*

Cisco 7600 Series
interface *type number*

Note: The number format varies depending on the network module or line card type and the router's chassis slot it is installed in. Refer to the appropriate hardware manual for numbering information

Cisco 7600 Series with Ports on Ethernet Service Cards
interface type *slot/bay/port* **access**

Note: The syntax may vary depending on the Ethernet service line card type. Refer to the appropriate hardware manual for numbering information. For example, for the ES20 line card the syntax takes the following format:

Subinterface Syntax Forms in Global Configuration Mode

Cisco 7200 Series
interface *type slot/port* **.** *subinterface-number* [{**multipoint** | **point-to-point**}]

Cisco 7500 Series
interface *type slot/port-adapter* **.** *subinterface-number* [{**multipoint** | **point-to-point**}]

Cisco 7500 Series with Ports on VIP Cards
interface *type slot/port-adapter/port* **.** *subinterface-number* [{**multipoint** | **point-to-point**}]

Cisco ASR 901 Series Aggregation Services Routers
no interface *type number*

Shared Port Adapters
interface *type slot/subslot/port* [**.** *subinterface-number*]

Syntax Description

type	Type of interface to be configured. See the table below.
number	Port, connector, or interface card number. On Cisco 830 series routers, the *number*argumentspecifies the ethernet interface number. On Cisco 4700 series routers, the number argument specifies the network interface module (NIM) or network processor module (NPM) number. The numbers are assigned at the factory at the time of installation or when added to a system; they can be displayed with the **showinterfaces** command. For Cisco ASR 901 Series Aggregation Services Routers, the range is from 1 to 8.
name-tag	(Optional) Specifies the logic name to identify the server configuration so that multiple server configurations can be entered. This optional argument is for use with the Redundant Link Manager (RLM) feature.
slot	Chassis slot number. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide.

/ *voice-module-slot*	Voice module slot number. The slash(/)is required. Refer to the "Cisco 3700 Series Routers Voice Interface Numbering" section of the "Understanding Interface Numbering and Cisco IOS Basics" chapter in the platform-specific SPA software configuration guide.
/ *voice-interface-slot*	Voice interface slot number. The slash(/)is required. Refer to the "Cisco 3700 Series Routers Voice Interface Numbering" section of the "Understanding Interface Numbering and Cisco IOS Basics" chapter in the platform-specific SPA software configuration guide.
/ *subslot*	Secondary slot number on a SIP where a SPA is installed. The slash (/) is required. Refer to the platform-specific SPA hardware installation guide and the corresponding "Specifying the Interface Address on a SPA" topic in the platform-specific SPA software configuration guide for subslot information.
/ *unit*	Number of the daughter card on the network module. For analysis module and content engine (CE) network modules, always use 0. Theslash(/)is required.
/bay	Card interface bay number in a slot. Theslash(/)is required. Refer to the appropriate hardware manual for bay information.
/ *port*	Port or interface number. Theslash(/)is required. Refer to the appropriate hardware manual for port information. For SPAs, refer to the corresponding "Specifying the Interface Address on a SPA" topics in the platform-specific SPA software configuration guide.
router-shelf	Router shelf number in a Cisco AS5800 universal access server. Refer to the appropriate hardware manual for router shelf information.
: *channel-group*	Channel group number. Cisco 7500 series routers specify the channel group number in the range of 0 to 4 defined with the **channel-group** controller configuration command.
/ *port-adapter*	Port adapter number. Refer to the appropriate hardware manual for information about port adapter compatibility. Theslash(/) is required.
. *subinterface-number*	Subinterface number in the range 1 to 4294967293. The number that precedes the period (.) must match the number to which this subinterface belongs.
access	Creates an access interface for an IP subscriber. The access interface is configured as a subinterface of the physical interface that the IP subscriber is connected to.
multipoint | **point-to-point**	(Optional) Specifies a multipoint or point-to-point subinterface. There is no default .

Command Default

No interface types are configured.

Command Modes

Global configuration (config)

RITE configuration (config-rite)

Note To use this command with the RLM feature, the networking device must be in interface configuration mode.

Command History

Release	Modification
10.0	This command was introduced for the Cisco 7000 series routers.
11.0	This command was implemented on the Cisco 4000 series routers.
12.0(3)T	The optional *name-tag*argument was added for the RLM feature.
12.2(13)T	The **content-engine** keyword was added.
12.2(15)T	The **lex** keyword was removed because the LAN Extension feature is no longer available in Cisco IOS software.
12.2(20)S2	This command was implemented for SPAs on the Cisco 7304 router.
12.3(4)T	The **serviceengine** keyword was added. Support was added for the **interface** command to be used in RITE configuration mode to support IP trfaffic export profiles.
12.3(7)T	The **analysis-module** keyword was added.
12.2(22)S	Support for RITE configuration mode and IP traffic export profiles was added.
12.3(14)T	The **satellite** keyword was added to support satellite interface configuration on network modules.
12.2(18)SXE	This command was implemented for SPAs on the Cisco 7600 series routers and Catalyst 6500 series switches.
12.0(31)S	This command was implemented for SPAs on the Cisco 12000 series routers.
12.2(18)SXF	The **tengigabitethernet** keyword was added for support of the10 Gigabit Ethernet interface type.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE 2.1	This command was implemented on Cisco ASR 1000 series routers.
15.1(2)SNG	This command was implemented on Cisco ASR 901 Series Aggregation Services Routers.
Cisco IOS XE Release 3.9S	This command was implemented on Cisco 4400 Series ISR.
15.2(02)SA	This command was implemented on Cisco ME 2600X Series Ethernet Access Switches.
15.1(2)SNG	This command was implemented on Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

This command does not have a **no** form except for Cisco ASR 901 Series Aggregation Services Routers.

The table below displays the keywords that represent the types of interfaces that can be configured with the **interface** command. Replace the *type* argument with the appropriate keyword from the table.

Table 20: Interface Type Keywords

Keyword	Interface Type
analysis-module	Analysis module interface. The analysis module interface is a Fast Ethernet interface on the router that connects to the internal interface on the Network Analysis Module (NAM). This interface cannot be configured for subinterfaces or for speed, duplex mode, and similar parameters. See the command-line interface (CLI) help for a list of valid parameters.
async	Port line used as an asynchronous interface.
atm	ATM interface.
bri	ISDN BRI. This interface configuration is propagated to each of the B channels. B channels cannot be individually configured. The interface must be configured with dial-on-demand commands in order for calls to be placed on that interface.
content-engine	Content engine (CE) network module interface. The CE network module interface cannot be configured for subinterfaces or for speed, duplex mode, and similar parameters. See the command-line interface (CLI) help for a list of valid parameters. **Note** The **content-engine** keyword was formerly documented as the **interfacecontent-engine** command.
dialer	Dialer interface.
ethernet	Ethernet IEEE 802.3 interface.
fastethernet	100-Mbps Ethernet interface. In RITE configuration mode, specifies the outgoing (monitored) interface for exported IP traffic. **Note** The **fastethernet** keyword was formerly documented as the **interfacefastethernet** command.
fddi	FDDI interface.
gigabitethernet	1000-Mbps Ethernet interface. **Note** The **gigabitethernet** keyword was formerly documented as the **interfacegigabitethernet** command.
group-async	Master asynchronous interface. **Note** The **group-async** keyword was formerly documented as the **interfacegroup-async** command.
hssi	High-Speed Serial Interface (HSSI).

Keyword	Interface Type
loopback	Software-only loopback interface that emulates an interface that is always up. It is a virtual interface supported on all platforms. The *number* argument is the number of the loopback interface that you want to create or configure. There is no limit on the number of loopback interfaces that you can create.
null	Null interface.
port-channel	Port channel interface. **Note** The **port-channel** keyword was formerly documented as the **interfaceport-channel** command.
pos	Packet OC-3 interface on the Packet-over-SONET (POS) interface processor. **Note** The **pos** keyword was formerly documented as the **interfacepos** command.
Satellite	Satellite network module. Enters satellite configuration mode.
sdcc	Section data communications channel interface.
serial	Serial interface.
service-engine	Network module (NM) or an Advanced Integration Module (AIM), this command may be used for NMs and AIMs only. If your system does not have this hardware, you will be unable to enter this command. The no form of this command (no interface service-engine) is not available. The exit command can be used to exit interface configuration mode.
switch	Switch interface.
tengigabitethernet	10-Gigabit Ethernet interface.
tokenring	Token Ring interface.
tunnel	Tunnel interface; a virtual interface. The *number* argument is the number of the tunnel interface that you want to create or configure. There is no limit on the number of tunnel interfaces that you can create.
vg-anylan	100VG-AnyLAN port adapter. **Note** The **vg-anylan** keyword was formerly documented as the **interfacevg-anylan** command.

Creating an IP Traffic Export Profile

Ip traffic export is intended only for software switching platforms; distributed architectures are not supported.

After you configure an IP traffic export profile using the **iptraffic-exportprofile**global configuration command, you must also include the **interface**command after the **iptraffic-exportprofile**command; otherwise, the profile will be unable to export the captured IP packets. If you do not use the **interface** command, you will receive a warning that indicates that the profile is incomplete.

Subinterfaces

Subinterfaces can be configured to support partially meshed Frame Relay networks. Refer to the “Configuring Serial Interfaces” chapter in the *CiscoIOSInterfaceandHardwareComponentConfigurationGuide*.

Using the analysis-module Keyword

The analysis module interface is used to access the NAM console for the initial configuration. After the NAM IP parameters are configured, the analysis module interface is typically used only during NAM software upgrades and while troubleshooting if the NAM Traffic Analyzer is inaccessible.

Visible only to the Cisco IOS software on the router, the analysis module interface is an internal Fast Ethernet interface on the router that connects to the internal NAM interface. The analysis module interface is connected to the router’s Peripheral Component Interconnect (PCI) backplane, and all configuration and management of the analysis module interface must be performed from the Cisco IOS CLI.

Using the group-async Keyword

Using the **group-async** keyword, you create a single asynchronous interface with which other interfaces are associated as members using the **group-range**command. This one-to-many configuration allows you to configure all associated member interfaces by entering one command on the group master interface, rather than entering this command on each individual interface. You can create multiple group masters on a device; however, each member interface can be associated only with one group.

Using the port-channel Keyword

The Fast EtherChannel feature allows multiple Fast Ethernet point-to-point links to be bundled into one logical link to provide bidirectional bandwidth of up to 800 Mbps. You can configure the port-channel interface as you would any Fast Ethernet interface.

After you create a port-channel interface, you assign upto four Fast Ethernet interfaces to it. For information on how to assign a Fast Ethernet interface to a port-channel interface, refer to the **channel-group** command in the interface configuration mode.

Caution The port-channel interface is the routed interface. Do not enable Layer 3 addresses on the physical Fast Ethernet interfaces. Do not assign bridge groups on the physical Fast Ethernet interfaces because doing so creates loops. Also, you must disable spanning tree.

Caution With Release 11.1(20)CC, the Fast EtherChannel supports Cisco Express Forwarding (CEF) and distributed Cisco Express Forwarding (dCEF). We recommend that you clear all explicit**iproute-cachedistributed** commands from the Fast Ethernet interfaces before enabling dCEF on the port-channel interface. Clearing the route cache gives the port-channel interface proper control of its physical Fast Ethernet links. When you enable CEF/dCEF globally, all interfaces that support CEF/dCEF are enabled. When CEF/dCEF is enabled on the port-channel interface, it is automatically enabled on each of the Fast Ethernet interfaces in the channel group. However, if you have previously disabled CEF/dCEF on the Fast Ethernet interface, CEF/dCEF is not automatically enabled. In this case, you must enable CEF/dCEF on the Fast Ethernet interface.

As you work with the **port-channel**keyword, consider the following points:

- Currently, if you want to use the Cisco Discovery Protocol (CDP), you must configure it only on the port-channel interface and not on the physical Fast Ethernet interface.

- If you do not assign a static MAC address on the port-channel interface, the Cisco IOS software automatically assigns a MAC address. If you assign a static MAC address and then later remove it, Cisco IOS software automatically assigns a MAC address.
- The **access** keyword creates an ethernet channel access interface for an IP subscriber and is specific to Cisco 7600 series routers only. For more information on access interface, see IP Subscriber Interfaces.

Using the vg-anylan Keyword

The 100VG-AnyLAN port adapter provides a single interface port that is compatible with and specified by IEEE 802.12. The 100VG-AnyLAN port adapter provides 100 Mbps over Category 3 or Category 5 cable with RJ-45 terminators and supports IEEE 802.3 Ethernet packets.

You configure the 100VG-AnyLAN port adapter as you would any Ethernet or Fast Ethernet interface. The 100VG-AnyLAN port adapter can be monitored with the IEEE 802.12 Interface MIB.

Cisco ASR 901 Series Aggregation Services Routers

The first EtherChannel interface configured becomes the bundled master for all EtherChannel interfaces in the group. That is, the MAC address of the first EtherChannel interface is the MAC address for all EtherChannel interfaces in the group. If the first EtherChannel interface is removed at any time, the second EtherChannel interface becomes the bundled master by default.

Repeat this configuration on every EtherChannel port to be bundled into a Fast Ether Channel (FEC) or Gigabit Ether Channel (GEC) group. This configuration must be present on all EtherChannel interfaces before the EtherChannel group can be configured.

Cisco 4400 Series Integrated Services Router (ISR)

The Gigabit Ethernet interface allows you to perform management tasks on the router and is often referred as the management interface port. You can use the Gigabit Ethernet interface to access the router via Telnet and SSH to perform management tasks on the router. The interface is most useful before a router has begun routing, or in troubleshooting scenarios when other forwarding interfaces are inactive. You can configure a Gigabit Ethernet interface on your router using the **interface GigabitEthernet0** command in Global configuration mode.

Analysis Module Interface with NAM Router: Example

The following example configures an analysis module interface when the NAM router is in router slot 1:

```
Router(config)# interface analysis-module 1/0
```

Asynchronous Group Master Interface: Example

The following example shows how to define asynchronous group master interface 0:

```
Router(config)# interface group-async 0
```

Content Engine Network Module Interface: Example

The following example configures an interface for a content engine network module in slot 1:

```
Router(config)# interface content-engine 1/0
```

Ethernet Interface on Cisco 830 Router: Example

The following example configures a new **ethernet2**interface on the LAN or on the WAN side of the Cisco 830 series router.

```
c837# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
c837(config)# interface ethernet 2
```

Ethernet Port on Ethernet Interface Processor on Cisco 7500 Series Router: Example

The following example shows how to configure Ethernet port 4 on the Ethernet Interface Processor (EIP) in slot 2 on the Cisco 7500 series router:

```
Router(config)# interface ethernet 2/4
```

Exporting IP Traffic (RITE): Example

The following example shows how to configure the profile “corp1,” which will send captured IP traffic to host “00a.8aab.90a0” at the interface “FastEthernet 0/1.” This profile is also configured to export one in every 50 packets and to allow incoming traffic only from the access control list “ham_ACL.”

```
Router(config)# ip traffic-export profile corp1
Router(config-rite)# interface FastEthernet 0/1
Router(config-rite)# bidirectional
Router(config-rite)# mac-address 00a.8aab.90a0
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp1
```

Fast Ethernet Interface on Cisco 2600 Router: Example

The following example shows how to configure Fast Ethernet interface 0 on a Cisco 2600 series router:

```
Router(config)# interface fastethernet0/0
```

or

```
Router(config)# interface fastethernet0/0.1
```

Fast Ethernet Interface on Cisco 3600 Router: Example

The following example shows how to configure Fast Ethernet interface 0 on a Cisco 3600 series router:

```
Router(config)# interface fastethernet0/0
```

or

```
Router(config)# interface fastethernet0/0.1
```

Fast Ethernet Interface with ARPA Encapsulation on Cisco 4700 Router: Example

The following example shows how to configure Fast Ethernet interface 0 for standard ARPA encapsulation (the default setting) on a Cisco 4700 series router:

```
Router(config)# interface fastethernet 0
```

Fast Ethernet Interface on Cisco 7100 Router: Example

The following example shows how to configure Fast Ethernet interface 0 on a Cisco 7100 series router:

```
Router(config)# interface fastethernet0/0
```

or

```
Router(config)# interface fastethernet0/0.1
```

Fast Ethernet Interface on Cisco 12000 Router: Example

The following example shows how to configure Fast Ethernet interface 6 on a Cisco 12000 series router:

```
Router(config)# interface fastethernet6/0
```

or

```
Router(config)# interface fastethernet6/0.1
```

Gigabit Ethernet Interface: Example

The following example shows how to configure the Gigabit Ethernet interface for slot 0, port 0:

```
Router(config)# interface gigabitethernet 0/0
```

Gigabit Ethernet Interface on Cisco 4400 Series ISR: Example

The following example shows how to configure the Gigabit Ethernet Interface. The Gigabit Ethernet Interface or the management port is always GigabitEthernet0.

```
Router# config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet0
Router(config-if)#
```

Gigabit Ethernet Interface on Cisco uBR10012 Router: Example

The following example shows how to specify the second interface (1) on a Gigabit Ethernet SPA installed in the first subslot of a SIP (0) installed in chassis slot 3:

```
Router(config)# interface gigabitethernet 3/0/1
```

Loopback Interface: Example

The following example shows how to enable loopback mode and assign an IP network address and network mask to the interface. The loopback interface established here will always appear to be up.

```
Router(config)# interface loopback 0
Router(config-if)# ip address 10.108.1.1 255.255.255.0
```

Packet over SONET Interface: Example

The following example shows how to specify the single Packet OC-3 interface on port 0 of the POS OC-3 port adapter in slot 2:

```
Router(config)# interface pos 2/0
```

Partially Meshed Frame Relay Network: Example

The following example shows how to configure a partially meshed Frame Relay network. In this example, subinterface serial 0.1 is configured as a multipoint subinterface with two associated Frame Relay permanent virtual connections (PVCs), and subinterface serial 0.2 is configured as a point-to-point subinterface.

```
Router(config)# interface serial 0
Router(config-if)# encapsulation frame-relay
Router(config-if)# exit
Router(config)# interface serial 0/0.1 multipoint
Router(config-if)# ip address 10.108.10.1 255.255.255.0
Router(config-if)# frame-relay interface-dlci 42 broadcast
Router(config-if)# frame-relay interface-dlci 53 broadcast
Router(config-if)# exit
Router(config)# interface serial 0/0.2 point-to-point
```

```
Router(config-if)# ip address 10.108.11.1 255.255.255.0
Router(config-if)# frame-relay interface-dlci 59 broadcast
```

Port Channel Interface: Example

The following example shows how to create a port-channel interface with a channel group number of 1 and add two Fast Ethernet interfaces to port-channel 1:

```
Router(config)# interface port-channel 1
Router(config-if)# ip address 10.1.1.10 255.255.255.0
Router(config-if)# exit
Router(config)# interface fastethernet 1/0/0
Router(config-if)# channel-group 1
Router(config-if)# exit
Router(config)# interface fastethernet 4/0/0
Router(config-if)# channel-group 1
```

SDCC Interface on a POS Shared Port Adapter: Example

The following example configures the first interface (port 0) as a section data communications channel (SDCC) interface on a POS SPA, where the SPA is installed in the top subslot (0) of the MSC, and the MSC is installed in slot 4 of the Cisco 7304 router:

```
Router(config)# interface sdcc 4/3/0
Router(config-if)# ip address 10.1.9.2 255.255.255.0
Router(config-if)# logging event link-status
Router(config-if)# load-interval 30
Router(config-if)# no keepalive
Router(config-if)# no fair-queue
Router(config-if)# no cdp enable
```

Serial Interface with PPP Encapsulation: Example

The following example shows how to configure serial interface 0 with PPP encapsulation:

```
Router(config)# interface serial 0
Router(config-if)# encapsulation ppp
```

Shared Port Adapter Interface: Example

The following example configures the second interface (port 1) on a 4-Port 10/100 Fast Ethernet SPA for standard ARPA encapsulation (the default setting), where the SPA is installed in the bottom subslot (1) of the MSC, and the MSC is installed in slot 2 of the Cisco 7304 router:

```
Router(config)# interface fastethernet 2/1/1
```

T1 Serial Interface: Example

The following example shows how to configure circuit 0 of a T1 link for PPP encapsulation:

```
Router(config)# controller t1 4/1
Router(config-controller)# circuit 0 1
Router(config-controller)# exit
Router(config)# interface serial 4/1:0
Router(config-if)# ip address 10.108.13.1 255.255.255.0
Router(config-if)# encapsulation ppp
```

Token Ring Interface Processor: Example

The following example shows how to configure the Token Ring interface processor in slot 1 on port 0 of a Cisco 7500 series router:

```
Router(config)# interface tokenring 1/0
```

100VG-AnyLAN Interface: Example

The following example shows how to specify the 100VG-AnyLAN port adapter in the first port adapter in slot 1:

```
Router(config)# interface vg-anylan 1/0/0
```

Related Commands

Command	Description
channel-group	Defines the time slots that belong to each T1 or E1 circuit.
channel-group (Fast EtherChannel)	Assigns a Fast Ethernet interface to a Fast EtherChannel group.
clear interface	Resets the hardware logic on an interface.
controller	Configures an E1, J1, T1, or T3 controller and enters controller configuration mode.
group-range	Creates a list of asynchronous interfaces that are associated with a group interface on the same device.
ip traffic-export profile	Create or edit an IP traffic export profile.
mac-address	Sets the MAC layer address.
ppp	Starts an asynchronous connection using PPP.
show controllers content-engine	Displays controller information for CE network modules.
show interfaces	Displays information about interfaces.
show interfaces	Displays information about interfaces.
show interfaces content-engine	Displays basic interface configuration information for a CE network module.
shutdown (RLM)	Shuts down all of the links under the RLM group.

Command	Description
slip	Starts a serial connection to a remote host using SLIP.

interface analysis-module

To configure the Analysis-Module interface on the router that connects to an installed Network Analysis Module (NM-NAM), use the **interfaceanalysis-module** command in global configuration mode. This command does not have a not form.

interface analysis-module *slot/unit*

Syntax Description

slot	Number of the router chassis slot for the network module.
/ *unit*	Number of the daughter card on the network module. For NM-NAM, always use 0. The slash (/) between the slot and unit arguments is required.

Command Default

The interface is not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced on the following platforms: Cisco 2600XM series, Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.3(8)T4	This command was implemented on the following platforms: Cisco 2811, Cisco 2821, and the Cisco 2851 series.
12.3(11)T	This command was made available on the Cisco 3800 series.

Usage Guidelines

The Analysis-Module interface is a Fast Ethernet interface on the router that connects to the internal interface on the Network Analysis Module (NM-NAM).

This type of interface cannot be configured for subinterfaces or for speed, duplex mode, and similar parameters. See the command-line interface (CLI) help for a list of valid parameters.

The **interfaceanalysis-module**command enters Analysis-Module interface configuration mode.

Examples

The following example shows how to configure the Analysis-Module interface when the NM-NAM is in router slot 1:

```
Router(config)# interface analysis-module 1/0
```

Related Commands

Command	Description
ip unnumbered	Enables IP processing on an interface without assigning an explicit IP address to the interface.
show interfaces analysis-module	Displays status, traffic data, and configuration information about the Analysis-Module interface.

interface content-engine

The **interfacecontent-engine**command is now documented as the **content-engine**keyword of the **interface** command. For more information, see the **interface**command.

interface fastethernet

The **interfacefastethernet**command is now documented as the **fastethernet**keyword of the **interface** command. For more information, see the **interface** command.

interface gigabitethernet

The **interfacegigabitethernet**command is now documented as the **gigabitethernet**keyword of the **interface** command. For more information, see the interface command.

interface group-async

The **interfacegroup-async**command is now documented as the **group-async**keyword of the **interface** command. For more information, see the **interface** command.

interface integrated-service-engine

To configure the Cisco wireless LAN controller network module (WLCM) interface with dot1q encapsulation on the router, use the **interfaceintegrated-service-engine** command.

interface integrated-service-engine slot/unit

Syntax Description

slot/unit	Specifies the router slot and unit numbers for the WLCM.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.

Examples

The following example shows how to create dot1Q virtual LAN (VLAN) subinterfaces under the **interfaceintegrated-service-engine** command:

```
Router(config)# interface integrated-service-engine
 1/0
Router(config-if)# exit
Router(config)# interface integrated-service-engine
 1/0.10
Router(config-subif)# encapsulation dot1q
 10

If the interface doesn't support baby giant frames
maximum mtu of the interface has to be reduced by 4
bytes on both sides of the connection to properly
transmit or receive large packets. Please refer to
documentation on configuring IEEE 802.1Q vLANs.

Router(config-subif)# end
```

Related Commands

show interfaces integrated-service-engine

interface ism

To configure an interface on the router that connects to an internal service module (ISM), use the **interfaceism** command in global configuration mode. This command does not have a no form.

interface ism *slot/port*

Syntax Description

slot	Router slot in which the service module is installed. For internal service modules, always use 0.
/ *port*	Port number of the module interface. Range: 0 or 1. The slash mark (/) is required.

Command Default

The interface is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

This command enters interface configuration mode to configure the interface between the router and the ISM or between the ISM and Multi-Gigabit Fabric (MGF).

Examples

The following example shows how to enter interface configuration mode for the ISM:

```
Router(config)# interface ism 0/0
```

Related Commands

Command	Description
ip unnumbered	Enables IP processing on an interface without assigning an explicit IP address to the interface.
service-module ip address	Specifies the IP address of the module side of the interface.
show interfaces ism	Displays status, traffic data, and configuration information about the ISM interface.

interface port-channel

The **interfaceport-channel** command is now documented as the **port-channel**keyword of the **interface** command. For more information, see the **interface** command.

interface pos

The **interfacepos** command is now documented as the **pos**keyword of the **interface** command. For more information, see the **interface**command.

interface range

To execute commands on multiple subinterfaces at the same time, use the **interfacerange** command in global configuration mode.

interface range {*type number* [[-**interface** *number*]] [,]... *type number* | **macro** *word*}
no interface range *type number*

Syntax Description

type number	Interface type and interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function. • You can enter any number of interface type and numbers.
- *interface-number*	(Optional) Ending interface number.
,	Allows you to configure more interface types.
macro	Specifies a macro keyword.
word	Previously defined keyword, up to 32 characters long.

Command Default

No interface range is set.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XE	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(2)DD	This command was expanded to support subinterface ranges.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(18)SX	This command was integrated into Cisco IOS Release 12.2(18)SX.
12.2(33)SXH	The **create** keyword was added to enable the creation of VLANs that operate within a specified range of physical interfaces.

Usage Guidelines

Configuration Changes

All configuration changes made to a range of subinterfaces are saved to NVRAM, but the range itself does not get saved to NVRAM. Use the **defineinterfacerange** command to create and save a range.

You can enter the range in two ways:

- Specifying up to five interface ranges

- Specifying a previously defined macro

You can specify either the interfaces or the name of a range macro. A range must consist of the same interface type, and the interfaces within a range cannot span slots.

You cannot specify both the **interfacerange**and **macro** keywords in the same command. After creating a macro, the command does not allow you to enter additional ranges. Likewise, if you have already specified an interface range, the command does not allow you to enter a macro.

The spaces around the hyphen in the **interfacerange** command syntax are required. For example, using a Catalyst 6500 router, the command **interfacerangefastethernet1-6**is valid; the command **interfacerangefastethernet1-6**is not valid.

VLANs

When you define a Catalyst VLAN, valid values are from 1 to 4094. The last VLAN number cannot exceed 4094.

You cannot use the **interfacerange** command to create switch virtual interfaces (SVIs) in that particular range. You can use the **interfacerange** command only to configure existing VLAN SVIs within the range. To display VLAN SVIs, enter the **showrunning-config** command. VLANs not displayed cannot be used in the **interfacerange** command.

The commands entered under the**interfacerange** command are applied to all existing VLAN SVIs within the range.

You can enter the command **interfacerangecreatevlan***x-y* to create all VLANs in the specified range that do not already exist. If you are using discontiguous VLANs, you can use the **interfacerangevlan** command to configure multiple SVIs without creating unneeded SVIs and wasting interface descriptor blocks (IDBs).

After specifying a VLAN range, you can continue using the **interfacerange** command to specify another interface (**ATM**, **FastEthernet**, **GigabitEthernet**, **loopback**, **port-channel**, or **tunnel**).

Examples

interface range Fast Ethernet Examples

The following example shows how to use the **interfacerange** command to configure a Fast Ethernet range:

```
Router(config)# interface range fastethernet 5/1 - 4
```

The following example configures the Fast Ethernet subinterfaces within the range 5/1.1 to 5/1.4 and applies the following VLAN IDs to those subinterfaces:

```
Fast Ethernet5/1.1 = VLAN ID 301 (vlan-id)
Fast Ethernet5/1.2 = VLAN ID 302 (vlan-id = 301 + 2 - 1 = 302)
Fast Ethernet5/1.3 = VLAN ID 303 (vlan-id = 301 + 3 - 1 = 303)
Fast Ethernet5/1.4 = VLAN ID 304 (vlan-id = 301 + 4 - 1 = 304)
Router(config)# interface range fastethernet 5/1 - 4

Router(config-if-range)# encapsulation dot1q 301
Router(config-if-range)# no shutdown

Router(config-if)#
*Oct  6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/1.1, changed state to up
*Oct  6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/1.2, changed state to up
*Oct  6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/1.3, changed state to up
```

```
*Oct  6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/1.4, changed state to up
*Oct  6 08:24:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/1.1, changed
 state to up
*Oct  6 08:24:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/1.2, changed
 state to up
*Oct  6 08:24:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/1.3, changed
 state to up
*Oct  6 08:24:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/1.4, changed
 state to up
```

interface range Gigabit Ethernet Example

The following example shows how to set a Gigabit Ethernet range:

```
Router(config)# interface range gigabitethernet 1/1 - 6
```

interface range Loopback Example

The following example shows how to use the loopback interface:

```
Router(config)# interface range loopback 34567
```

interface range Tunnel Example

The following example shows how to use the tunnel interface:

```
Router(config)# interface range tunnel 55555
```

interface range Port Channel Example

The following example shows how to use the port-channel interface:

```
Router(config)# interface range port-channel 100
```

interface range VLAN Examples

The following example shows how to set a VLAN:

```
Router(config)# interface range vlan 123
```

The following example shows how to create a range of VLANs:

```
Router(config)# interface range create vlan 4
```

interface range macro Example

The following example shows how to execute a range macro:

```
Router(config)# interface range macro macro1
```

Related Commands

Command	Description
define interface range	Defines an interface range macro.
encapsulation dot1q	Applies a unique VLAN ID to each subinterface within the range.
interface vlan	Configures a VLAN interface.

interface satellite

To enter satellite interface configuration mode, use the **interfacesatellite** command in global configuration mode.

interface satellite *slot*/*unit*

Syntax Description

slot	Router chassis slot in which the network module is installed.
unit	Interface number. For NM-1VSAT-GILAT network modules, always use 0.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Examples

The following example shows how to enter satellite interface configuration mode:

```
Router(config)# interface satellite 1/0
Router(config-if)#
```

Related Commands

Command	Description
service-module satellite status	Displays status information related to the hardware and software on the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT), including the initial configuration parameters.
show controllers satellite	Displays controller information about the internal router interface that connects to an installed Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT).
show interface satellite	Displays general interface settings and traffic rates for the internal router interface that connects to an installed Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT).

interface service-engine

To enter the interface configuration mode for a network module (NM) or an advanced Integration Module (AIM), use the **interfaceservice-engine** command in global configuration mode.

interface service-engine *slot/port*

Syntax Description

slot	Interface slot number.
port	Interface port number.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)ZJ	This command was introduced for NMs.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(7)T	Support was added for AIMs.

Usage Guidelines

This command may only be used for NMs and AIMs. If your system does not have this hardware, then you will be unable to enter this command.

The **no** form of this command (**nointerfaceservice-engine**) is not available. The **exit** command can be used to exit the interface configuration mode.

Examples

The following example shows the command for entering configuration mode for either a NM or AIM located in slot 1, unit 1:

```
Router (config)# interface service-engine 1/1
Router (config-if)# exit
```

interface sm

To configure an interface on the router that connects to an SM-SRE service module, use the **interfacesm** command in global configuration mode. This command does not have a no form.

interface sm *slot/port*

Syntax Description

slot	Router slot in which the service module is installed. Range: 1 to 4.
/ *port*	Port number of the module interface. Range: 0 or 1. The slash mark (/) is required.

Command Default

The interface is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

This command enters interface configuration mode to configure the interface between the router and the service module or between the service module and Multi-Gigabit Fabric (MGF).

Examples

The following example shows how to enter interface configuration mode for the service module:

```
Router(config)# interface sm 1/0
```

Related Commands

Command	Description
ip unnumbered	Enables IP processing on an interface without assigning an explicit IP address to the interface.
service-module ip address	Specifies the IP address of the module side of the interface.
show interfaces sm	Displays status, traffic data, and configuration information about the service module interface.

interface vg-anylan

The **interfacevg-anylan** command is now documented as the **vg-anylan** keyword of the **interface** command. For more information, see the **interface**command.

interface vmi

To create a virtual multipoint interface (VMI) that can be configured and applied dynamically, use the**interfacevmi** command in global configuration mode. To remove a VMI interface, use the **no** form of this command.

interface vmi *interface-number*
no interface vmi *interface-number*

Syntax Description

interface-number	Number assigned to the VMI. The value range for VMI interface numbers is from 1 to 2147483647

Command Default

No VMI is defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)XF	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

VMI Interface Aggregation Point

The VMI interface acts as an aggregation point for multiple PPPoE connections from one or more radios over one or more physical interfaces.

OSPFv3 and EIGRP Route Advertisements

All OSPFv3, EIGRPv4, and EIGRPv6 route advertisements that are received over the PPPoE connections are reported to the routing protocol as coming from a single interface, thus simplifying the routing protocol topology table and providing scalability benefits of each of the routing protocols.

Examples

The following example shows how to create a VMI interface:

```
interface vmi 1
 ip address 10.2.1.1 255.255.255.0
 no ip redirects
 no ip split-horizon eigrp 1
 load-interval 30
 ipv6 address 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE/64
 ipv6 enable
 no ipv6 redirects
 ipv6 eigrp 1
 no ipv6 split-horizon eigrp 1
 physical-interface GigabitEthernet 0/0
 end
```

Related Commands

Command	Description
debug vmi	Displays debugging output for virtual multipoint interfaces (VMIs).

Command	Description
eigrp interface	Sets a threshold value to minimize hysteresis in a router-to-radio configuration.
mode bypass	Enables virtual multipoint interfaces (VMIs) to support multicast traffic.
physical interface	Creates a physical subinterface to be associated with the virtual multipoint interfaces (VMIs) on a router.

interface wlan-controller

To configure the Cisco Wireless Local Area Network (WLAN) controller network module interface with dot1q encapsulation on the router, use the **interfacewlan-controller** command in global configuration mode.

interface wlan-controller slot/unit

Syntax Description

slot/unit	Specifies the router slot and unit numbers for the WLAN controller network module.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
12.4(2)XA1	This command was introduced on the router software.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.

Examples

The following example shows how to create dot1Q virtual LAN (VLAN) subinterfaces under interface wlan-controller:

```
Router(config)# interface wlan-controller 1/0
Router(config-if)# exit
Router(config)# interface wlan-controller 1/0.10
Router(config-subif)# encapsulation dot1q 10

If the interface doesn't support baby giant frames
maximum mtu of the interface has to be reduced by 4
bytes on both sides of the connection to properly
transmit or receive large packets. Please refer to
documentation on configuring IEEE 802.1Q vLANs.

Router(config-subif)# end
```

international bit

To set the E3 international bit in the G.751 frame used by the PA-E3 port adapter, use the **internationalbit**command in interface configuration mode. To return to the default international bit, use the **no** form of this command.

international bit commandinternational bit {**0** | **1**} {**0** | **1**}
no international bit

Syntax Description

0	Sets either of the two required E3 international bits in the G.751 frame to 0. This is the default.
1	Sets either of the two required E3 international bits in the G.751 frame to 1.

Command Default

The default value for each bit is 0.

Command Modes

Interface configuration

Command History

Release	Modification
11.1 CA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **internationalbit** command sets bits 6 and 8, respectively, of set II in the E3 frame.

To verify the international bit configured on the interface, use the **showcontrollersserial** EXEC command.

Examples

The following example sets the international bit to 1 1 on the PA-E3 port adapter in slot 1, port adapter slot 0, interface 0:

```
Router(config)# interface serial 1/0/0
Router(config-if)# international bit 1 1
```

Related Commands

Command	Description
national bit (interface)	Sets the E3 national bit in the G.751 frame used by the PA-E3 port adapter.
show controllers serial	Displays information that is specific to the interface hardware.

inter-packet gap 6502-mode

To set the Inter-Packet Gap (IPG) value, use the **inter-packetgap6502-mode**command in interface configuration mode. To return to the default setting, use the **no** form of this command.

inter-packet gap 6502-mode
no inter-packet gap 6502-mode

Syntax Description

This command has no keywords or arguments.

Command Default

All fragments from flows that are received from an ACE with Layer 4 ports and permit action are permitted. All other fragments are dropped in the hardware. This action also applies to flows that are handled in the software regardless of this command setting.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXF5	This command was introduced on the Supervisor Engine 720.

Usage Guidelines

This command is supported only when a WS-X6704-10GE is connected to a WS-X6502-10GE. You enter this command to change the IPG value of the WS-X6704-10GE to match the IPG value of the WS-X6502-10GE.

The default 6704 mode sets the IPG value to average 12. Based on packet size, the IPG between successive packets ranges from 9 to 15.

The 6502 mode sets the IPG value to average 16. Based on packet size, the IPG between successive packets ranges from 13 to 19.

Examples

This example shows how to set the IPG to 6502 mode:

```
inter-packet gap 6502-mode
```

This example shows how to set the IPG to the default mode:

```
no inter-packet gap 6502-mode
```

invert data

To invert the data stream, use the **invertdata** command in interface configuration mode. This command applies only to the Cisco 7000 series routers with the RSP7000 and RSP7000CI, Cisco 7200 series routers, and Cisco 7500 series routers. To disable inverting the data stream, use the **no** form of this command.

invert data commandinvert data
no invert data

Syntax Description

This command has no arguments or keywords.

Command Default

Data is not inverted.

Command Modes

Interface configuration

Command History

Release	Modification
11.1CA	This command was introduced.
11.2P	This command was integrated into Cisco IOS Release 11.2 P.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

T1 Line Without B8ZS Encoding

If the interface on the PA-8T and PA-4T+ synchronous serial port adapters and the PA-T3 and PA-2T3 synchronous serial port adapters is used to drive a dedicated T1 line that does not have B8ZS encoding (a method to avoid 15 zeros), the data stream must be inverted (both transmitting and receiving data) either in the connecting CSU/DSU or in the interface.

Inverting is a method of avoiding excessive zeroes that is superseded by the use of B8ZS encryption. This option could be needed for use with legacy equipment that supports this option. By inverting the High-Level Data Link Control (HDLC) data stream, the HDLC zero insertion algorithm becomes a ones insertion algorithm that satisfies the T1 requirements. Be careful not to invert data both on the interface and on the CSU/DSU because two data inversions will cancel each other out.

AMI Line Coding

If the interface on the CT3IP uses alternate mark inversion (AMI) line coding, you must also invert the data on the T1 channel. For more information, see the **t1linecode**controller configuration command.

Examples

The following example inverts data on serial interface 3/1/0:

```
Router(config)# interface serial 3/1/0
Router(config-if)# invert data
```

Related Commands

Command	Description
t1 linecode	Specifies the type of linecoding used by the T1 channels on the CT3IP in Cisco 7500 series routers.

invert rxclock

To invert the phase of the receive (RX) clock signal on the universal I/O (UIO) serial interface that does not use the T1/E1 interface, use the **invertrxclock** command in interface configuration mode. To disable the phase inversion, use the **no** form of this command.

invert rxclock commandinvert rxclock
no invert rxclock

Syntax Description

This command has no arguments or keywords.

Command Default

The receive clock signal is not inverted.

Command Modes

Interface configuration

Command History

Release	Modification
11.3 MA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When a delay occurs between a signal being sent and the signal being received it can indicate that the receive clock signal is not appropriate for the interface rate. This command allows the receive clock signal to be inverted to attempt to correct the delay.

Examples

The following example inverts the receive clock signal on serial interface 1:

```
Router(config)# interface serial 1
Router(config-if)# invert rxclock
```

invert txclock

To invert the transmit (TX) clock signal, use the **inverttxclock** command in interface configuration mode. To return the TX clock signal to its initial state, use the **no** form of this command.

invert txclock
no invert txclock

Syntax Description

This command has no arguments or keywords.

Command Default

The transmit clock signal is not inverted.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
11.3	The **invert-transmit-clock** command was replaced by the **inverttxclock** command.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Delays between the serial clock transmit external (SCTE) clock and data transmission indicate that the TX clock signal might not be appropriate for the interface rate and length of cable being used. Different ends of the wire can have variances that differ slightly. The **inverttxclock** command compensates for these variances. This command replaces the **invert-transmit-clock** command.

Systems that use long cables or cables that are not transmitting the TxC signal (transmit echoed clock line, also known as TXCE or SCTE clock) can experience high error rates when operating at the higher transmission speeds. For example, if a PA-8T synchronous serial port adapter is reporting a high number of error packets, a phase shift might be the problem. Inverting the clock might correct this shift.

When a PA-8T or PA-4T+ port adapter interface is DTE, the **inverttxclock**command inverts the TxC signal it received from the remote DCE. When the PA-8T or PA-4T+ port adapter interface is DCE, this command changes the signal back to its original phase.

Examples

The following example inverts the TX clock signal on serial interface 3/0:

```
Router(config)# interface serial 3/0
Router(config-if)# invert txclock
```

ip dscp

To enable the use of IP differentiated services code point (DSCP) for packets that originate from a circuit emulation (CEM) channel, use the **ipdscp** command in CEM configuration mode. To disable the use of IP DSCP, use the **no** form of this command.

ip dscp [*dscp-value*]
no ip dscp

Syntax Description

dscp-value	(Optional) Value placed in the DSCP field of IP packets that originate from a CEM channel. Range is from 0 to 63. Default is 46.

Command Default

IP DSCP is enabled for packets that originate from a CEM channel.

Command Modes

CEM configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

DSCP is mutually exclusive from both IP type of service (ToS) and IP precedence. Thus, if DSCP is configured, the **iptos** command and the **ipprecedence** command are both unavailable at the command-line interface (CLI).

Examples

The following example shows how to set the IP DSCP field value to 36.

```
Router(config-cem)# ip dscp 36
```

Related Commands

Command	Description
ip precedence	Configures the IP precedence bits for the CEM channel.
ip tos	Configures the IP ToS bits for the CEM channel.

ip pxf

To manually enable the PXF processors, use the **ippxf** command in global configuration mode. To manually disable the PXF processors, use the **no** form of this command.

ip pxf
no ip pxf

Syntax Description

This command has no arguments or keywords.

Command Default

The PXF processors are enabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.1(9)EX	This command was introduced.
12.2(18)S	This command was introduced on Cisco 7304 routers running Cisco IOS Release 12.2(18)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The PXF processors are enabled by default. If they are ever disabled, you must enable them to take advantage of IP packet switching and feature acceleration. The PXF processors should never be disabled except for very short durations for debugging purposes.

Note You must also have IP Cisco Express Forwarding switching turned on for accelerated IP packet switching.

Examples

The following example enables the PXF processors:

```
ip pxf
```

Related Commands

Command	Description
show c7300 pxf accounting	Displays the number of packets entering or exiting the PXF processors.
show pxf accounting	Displays the PXF accounting.
show c7300 pxf interfaces	Displays the status of various interfaces known to the PXF processors.
show pxf interfaces	Displays a list of PXF interfaces.

ip rbscp ack-split

To configure the TCP ACK splitting feature of the Rate-Based Satellite Control Protocol (RBSCP) on an outgoing interface for packets that are permitted by a specified access list, use the **iprbscpack-split**command in interface configuration mode. To disable the feature on the interface, use the **no** form of this command.

ip rbscp ack-split *size* {*access-list-nameaccess-list-number*} **out**
no ip rbscp ack-split

Syntax Description

size	The number of TCP ACKs to send for every TCP ACK received. A *size*of 0 or 1 indicates that this feature is disabled (that is, no TCP ACK splitting will occur). The range is 0 through 32.
access-list-name | *access-list-number*	Standard or extended IP access list name or number that controls which packets are subject to TCP ACK splitting. That is, the feature is applied to packets that a **permit** statement allows; the feature is not applied to packets that a **deny** statement filters.
out	Specifies that this feature is applied to an outgoing interface.

Command Default

Disabled (TCP ACK splitting is not required on an outgoing interface for packets that are permitted by a specified acccess list).

Command Modes

Interface configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

This command enables TCP ACK splitting for outgoing packets that are permitted by the access list. TCP ACK splitting is a software technique to improve performance for clear-text TCP traffic using acknowledgment (ACK) splitting, in which a number of additional TCP ACKs are generated for each TCP ACK received.

TCP ACK splitting causes TCP to open the congestion window more quickly than usual, thus decreasing the effect of long latencies. TCP will generally open the congestion window by one maximum transmission unit (MTU) for each TCP ACK received. Opening the congestion window results in increased bandwidth becoming available. Configure this feature only when the satellite link is not using all the available bandwidth. Encrypted traffic cannot use TCP ACK splitting.

Caution Plan your network carefully so that no more than one Cisco IOS router in a given routing path has this feature enabled. You do not want to recursively ACK-split traffic.

An interface can use only one instance of this feature at a time. Each instance of this feature can be used on multiple interfaces.

If you configure this feature but it refers to a nonexistent access list, this is interpreted as having an access list that denies all traffic from being processed by the Access-List-Based RBSCP feature, so the feature is essentially disabled and the traffic goes through the normal switching path.

Examples

In the following example, the access list performs TCP ACK splitting on packets going out Ethernet interface 0 from a source at 172.22.18.5 to a destination at 172.23.27.4:

```
ip access-list extended satellite
 permit tcp 172.22.18.5 172.23.27.4
 exit
interface ethernet 0
 ip rbscp ack-split 6 satellite out
```

Related Commands

Command	Description
debug ip rbscp	Displays general error messages about access-list-based RBSCP.
debug ip rbscp ack-split	Displays information about TCP ACK splitting done in conjunction with RBSCP.

ip verify unicast source reachable-via

To enable Unicast Reverse Path Forwarding (Unicast RPF), use the **ip verify unicast source reachable-via** command in interface configuration mode. To disable Unicast RPF, use the **no** form of this command.

ip verify unicast source reachable-via {**any** | **rx** [**l2-src**]} [**allow-default**] [**allow-self-ping**] [*access-list*]
no ip verify unicast source reachable-via

Syntax Description

any	Examines incoming packets to determine whether the source address is in the Forwarding Information Base (FIB) and permits the packet if the source is reachable through any interface (sometimes referred to as loose mode).
rx	Examines incoming packets to determine whether the source address is in the FIB and permits the packet only if the source is reachable through the interface on which the packet was received (sometimes referred to as strict mode).
l2-src	(Optional) Enables source IPv4 and source MAC address binding.
allow-default	(Optional) Allows the use of the default route for RPF verification.
allow-self-ping	(Optional) Allows a router to ping its own interface or interfaces. **Caution** Use caution when enabling the **allow-self-ping** keyword. This keyword opens a denial-of-service (DoS) hole.
access-list	(Optional) Specifies a numbered access control list (ACL) in the following ranges: • 1 to 99 (IP standard access list) • 100 to 199 (IP extended access list) • 1300 to 1999 (IP standard access list, expanded range) • 2000 to 2699 (IP extended access list, expanded range)

Command Default

Unicast RPF is disabled.

Source IPv4 and source MAC address binding is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.1(CC), 12.0	This command was introduced. This command was not included in Cisco IOS Release 11.2 or 11.3.
12.1(2)T	Added access control list (ACL) support using the *access-list* argument. Added per-interface statistics on dropped or suppressed packets.

Release	Modification
12.0(15)S	This command replaced the **ip verify unicast reverse-path** command, and the following keywords were added: **allow-default**, **allow-self-ping**, **rx**, and **any**.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRC	This command was modified. The **l2-src** keyword was added to support the source IPv4 and source MAC address binding feature on platforms that support the Cisco Express Forwarding software switching path.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use the **ip verify unicast source reachable-via** interface command to mitigate problems caused by malformed or forged (spoofed) IP source addresses that pass through a router. Malformed or forged source addresses can indicate DoS attacks based on source IP address spoofing.

To use Unicast RPF, enable Cisco Express Forwarding or distributed Cisco Express Forwarding in the router. There is no need to configure the input interface for Cisco Express Forwarding. As long as Cisco Express Forwarding is running on the router, individual interfaces can be configured with other switching modes.

Note It is important for Cisco Express Forwarding to be configured globally on the router. Unicast RPF does not work without Cisco Express Forwarding.

Note Unicast RPF is an input function and is applied on the interface of a router only in the ingress direction.

When Unicast RPF is enabled on an interface, the router examines all packets that are received on that interface. The router checks to make sure that the source address appears in the FIB. If the **rx** keyword is selected, the source address must match the interface on which the packet was received. If the **any** keyword is selected, the source address must be present only in the FIB. This ability to "look backwards" is available only when Cisco Express Forwarding is enabled on the router because the lookup relies on the presence of the FIB. Cisco Express Forwarding generates the FIB as part of its operation.

Note If the source address of an incoming packet is resolved to a null adjacency, the packet will be dropped. The null interface is treated as an invalid interface by the new form of the Unicast RPF command. The older form of the command syntax did not exhibit this behavior.

Unicast RPF checks to determine whether any packet that is received at a router interface arrives on one of the best return paths to the source of the packet. If a reverse path for the packet is not found, Unicast RPF can drop or forward the packet, depending on whether an ACL is specified in the Unicast RPF command. If an ACL is specified in the command, when (and only when) a packet fails the Unicast RPF check, the ACL is checked to determine whether the packet should be dropped (using a deny statement in the ACL) or forwarded (using a permit statement in the ACL). Whether a packet is dropped or forwarded, the packet is counted in the global IP traffic statistics for Unicast RPF drops and in the interface statistics for Unicast RPF.

If no ACL is specified in the **ip verify unicast source reachable-via** command, the router drops the forged or malformed packet immediately, and no ACL logging occurs. The router and interface Unicast RPF counters are updated.

Unicast RPF events can be logged by specifying the logging option for the ACL entries that are used by the **ip verify unicast source reachable-via** command. Log information can be used to gather information about the attack, such as source address, time, and so on.

Strict Mode RPF

If the source address is in the FIB and reachable only through the interface on which the packet was received, the packet is passed. The syntax for this method is **ip verify unicast source reachable-via rx**.

Exists-Only (or Loose Mode) RPF

If the source address is in the FIB and reachable through any interface on the router, the packet is passed. The syntax for this method is **ip verify unicast source reachable-via any**.

Because this Unicast RPF option passes packets regardless of which interface the packet enters, it is often used on Internet service provider (ISP) routers that are "peered" with other ISP routers (where asymmetrical routing typically occurs). Packets using source addresses that have not been allocated on the Internet, which are often used for spoofed source addresses, are dropped by this Unicast RPF option. All other packets that have an entry in the FIB are passed.

allow-default

Normally, sources found in the FIB but only by way of the default route will be dropped. Specifying the **allow-default** keyword option will override this behavior. You must specify the **allow-default** keyword in the command to permit Unicast RPF to successfully match on prefixes that are known through the default route to pass these packets.

allow-self-ping

This keyword allows the router to ping its own interface or interfaces. By default, when Unicast RPF is enabled, packets that are generated by the router and destined to the router are dropped, thereby, making certain troubleshooting and management tasks difficult to accomplish. Issue the **allow-self-ping** keyword to enable self-pinging.

Caution Caution should be used when enabling the **allow-self-ping** keyword because this option opens a potential DoS hole.

Using RPF in Your Network

Use Unicast RPF strict mode on interfaces where only one path allows packets from valid source networks (networks contained in the FIB). Also, use Unicast RPF strict mode when a router has multiple paths to a given network, as long as the valid networks are switched through the incoming interfaces. Packets for invalid networks will be dropped. For example, routers at the edge of the network of an ISP are likely to have symmetrical reverse paths. Unicast RPF strict mode is applicable in certain multihomed situations, provided that optional Border Gateway Protocol (BGP) attributes, such as weight and local preference, are used to achieve symmetric routing.

Note With Unicast RPF, all equal-cost "best" return paths are considered valid. This means that Unicast RPF works in cases where multiple return paths exist, provided that each path is equal to the others in terms of the routing cost (number of hops, weights, and so on) and as long as the route is in the FIB. Unicast RPF also functions where Enhanced Internet Gateway Routing Protocol (EIGRP) variants are being used and unequal candidate paths back to the source IP address exist.

Use Unicast RPF loose mode on interfaces where asymmetric paths allow packets from valid source networks (networks contained in the FIB). Routers that are in the core of the ISP network have no guarantee that the best forwarding path out of the router will be the path selected for packets returning to the router.

IP and MAC Address Spoof Prevention

In Release 15.0(1)M and later, you can use the **l2-src**keyword to enable source IPv4 and source MAC address binding. To disable source IPv4 and source MAC address binding, use the **no** form of the **ip verify unicast source reachable-via**command.

If an inbound packet fails this security check, it will be dropped and the Unicast RPF dropped-packet counter will be incremented. The only exception occurs if a numbered access control list has been specified as part of the Unicast RPF command in strict mode, and the ACL permits the packet. In this case the packet will be forwarded and the Unicast RPF suppressed-drops counter will be incremented.

Note The **l2-src** keyword cannot be used with the loose uRPF command, **ip verify unicast source reachable-via any**command.

Not all platforms support the **l2-src** keyword. Therefore, not all the possible keyword combinations for strict Unicast RPF in the following list will apply to your platform:

Possible keyword combinations for strict Unicast RPF include the following:

```
allow-default
allow-self-ping
l2-src
<ACL-number>
allow-default allow-self-ping
allow-default l2-src
allow-default <ACL-number>
allow-self-ping l2-src
allow-self-ping <ACL-number>
l2-src <ACL-number>
allow-default allow-self-ping l2-src
allow-default allow-self-ping <ACL-number>
allow-default l2-src <ACL-number>
allow-self-ping l2-src <ACL-number>
allow-default allow-self-ping l2-src <ACL-number>
```

Examples

Single-Homed ISP Connection with Unicast RPF

The following example uses a very simple single-homed ISP connection to demonstrate the concept of Unicast RPF. In this example, an ISP peering router is connected through a single serial interface to one upstream ISP. Hence, traffic flows into and out of the ISP will be symmetric. Because traffic flows will be symmetric, a Unicast RPF strict-mode deployment can be configured.

```
ip cef
! or "ip cef distributed" for Route Switch Processor+Versatile Interface Processor-
(RSP+VIP-) based routers.
!
interface Serial5/0/0
 description - link to upstream ISP (single-homed)
 ip address 192.168.200.225 255.255.255.252
 no ip redirects
 no ip directed-broadcasts
 no ip proxy-arp
 ip verify unicast source reachable-via
```

ACLs and Logging with Unicast RPF

The following example demonstrates the use of ACLs and logging with Unicast RPF. In this example, extended ACL 197 provides entries that deny or permit network traffic for specific address ranges. Unicast RPF is configured on interface Ethernet 0/1/1 to check packets arriving at that interface.

For example, packets with a source address of 192.168.201.10 arriving at interface Ethernet 0/1/1 are dropped because of the deny statement in ACL 197. In this case, the ACL information is logged (the logging option is turned on for the ACL entry) and dropped packets are counted per-interface and globally. Packets with a source address of 192.168.201.100 arriving at interface Ethernet 0/1/2 are forwarded because of the permit statement in ACL 197. ACL information about dropped or suppressed packets is logged (the logging option is turned on for the ACL entry) to the log server.

```
ip cef distributed
!
int eth0/1/1
 ip address 192.168.200.1 255.255.255.0
 ip verify unicast source reachable-via rx 197
!
int eth0/1/2
 ip address 192.168.201.1 255.255.255.0
!
access-list 197 deny   ip 192.168.201.0 0.0.0.63 any log-input
access-list 197 permit ip 192.168.201.64 0.0.0.63 any log-input
access-list 197 deny   ip 192.168.201.128 0.0.0.63 any log-input
access-list 197 permit ip 192.168.201.192 0.0.0.63 any log-input
access-list 197 deny ip host 0.0.0.0 any log-input
access-list 197 deny ip 172.16.0.0 0.255.255.255 any log-input
access-list 197 deny ip 10.0.0.0 0.255.255.255 any log-input
access-list 197 deny ip 172.16.0.0 0.15.255.255 any log-input
access-list 197 deny ip 192.168.0.0 0.0.255.255 any log-input
```

MAC Address Binding on Software Switching Platforms Like the Cisco 7200 Series Routers

The following example shows how to enable source IPv4 and source MAC address binding on Ethernet 0/0:

```
Router# configure terminal
Router(config)# interface Ethernet0/0
Router(config-if)# ip address 10.0.0.1 255.255.255.0
Router(config-if)# ip verify unicast source reachable-via rx l2-src
```

Related Commands

Command	Description
ip cef	Enables Cisco Express Forwarding on the route processor card.
ip cef distributed	Enables Cisco Express Forwarding on the line card.

ipc buffers

To resize the interprocessor communication (IPC) buffer pool, use the **ipcbuffers** command in global configuration mode. To disable the configuration, use the **no** form of this command.

ipc buffers {**max-free** | **min-free** | **permanent**} *buffers*
no ipc buffers {**max-free** | **min-free** | **permanent**}

Syntax Description

max-free *buffers*	Specifies the maximum number of buffers that must be free. The range is from 8 to 10000.
min-free *buffers*	Specifies the minimum number of buffers that must be free. The range is from 1 to 17.
permanent *buffers*	Specifies the number of buffers that must be permanantly allocated for IPC apart from the buffers that are dynamically allocated and freed. The range is from 2 to 5000.

Command Default

The default buffer value is set by the platform during initialization.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
Cisco IOS XE Release 2.1	This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

You can use the **ipcbuffers** command when you would want to resize the buffer pool.

Examples

The following example shows how to set the maximum number of free buffers to 10:

```
Router(config)# ipc buffers max-free 10
```

Related Commands

Command	Description
ipc holdq threshold	Configures IPC holdq threshold values.
show ipc	Displays IPC statistics.

ipc header-cache

To resize the interprocess communication (IPC) permanent cache, use the **ipcheader-cache** command in global configuration mode. To disable the configuration, use the **no** form of this command.

ipc header-cache permanent *high-cache low-cache*
no ipc header-cache permanent

Syntax Description

permanent	Specifies the permanent IPC cache.
high-cache	Maximum permanent cache size. The range is from 1000 to 10000.
low-cache	Lower cache watermark. The range is from 100 to 2000.

Command Default

The default values are set by the platform during initialization.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
Cisco IOS XE Release 2.1	This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following example shows how to set the maximum permanent cache value to 1000 and lower cache value to 200 of an IPC server:

```
Router(config)# ipc header-cache permanent 1000 200
```

Related Commands

Command	Description
ipc holdq threshold	Configures IPC holdq threshold values.
show ipc	Displays IPC statistics.

ipc holdq threshold

To configure interprocessor communication (IPC) holdq threshold values, use the **ipcholdqthreshold**command in global configuration mode. To disable the configuration, use the **no** form of this command.

ipc holdq threshold {**lower** *start-threshold* | **upper** *stop-threshold*}
no ipc holdq threshold {**lower** | **upper**}

Syntax Description

lower	Specifies the lower threshold for IPC holdq.
start-threshold	Threshold to start sending IPC messages. The range is from 10 to 2000.
upper	Specifies the upper threshold for IPC holdq.
stop-threshold	Threshold to stop sending IPC messages. The range is from 40 to 4000.

Command Default

The default values threshold is set by the platform during initialization.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

The holdq OFF and ON thresholds are used to throttle the message sent based on the traffic at the driver. If the number of messages to be processed by the driver has increased than the OFF threshold, then the messages are not passed from the transport layer to the driver. The messages will be sent again once the count decreases below the ON threshold.

You can use the**ipcholdq**command when the driver message processing speed has decreased or increased to a greater extent than the specifications.

Examples

The following example shows how to configure a lower threshold value of 100 for IPC holdq:

```
Router(config)# ipc holdq threshold lower 100
```

Related Commands

Command	Description
ipc buffers	Resizes the IPC buffer pool.
show ipc	Displays IPC statistics.

ipc master

To configure the IP address of the interprocessor communication (IPC) master server, use the **ipcmaster** command in global configuration mode. To disable the configuration, use the **no** form of this command.

ipc master {*ip-address* | **self**}
no ipc master

Syntax Description

ip-address	IP address of the master server.
self	Assigns the host as the IPC master server.

Command Default

IP address is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Examples

The following example shows how to configure 192.0.2.1 as the IP address of the master server:

```
Router(config)# ipc master 192.0.2.1
```

Related Commands

Command	Description
ipc buffers	Resizes the IPC buffer pool.
show ipc	Displays IPC statistics.

ipc zone default

To enter interprocess communication (IPC) zone configuration mode, use the **ipczonedefault**command in global configuration mode. To remove a previously configured association, use the **no** form of this command.

ipc zone default
no ipc zone default

Syntax Description

This command has no arguments or keywords.

Command Default

The user is not in IPC zone configuration mode.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

The **ipczonedefault** command places the router into IPC zone configuration mode. In this mode, the user can configure the default IPC zone.

The **no** form of the **ipczonedefault** command removes any previously configured association.

Examples

The following example places the router into IPC zone configuration mode:

```
Router(config)# ipc zone default
Router(config-ipczone)#
```

Related Commands

Command	Description
show ipc	Displays IPC statistics.

iphc-profile

To create an IP Header Compression (IPHC) profile and to enter IPHC-profile configuration mode, use the **iphc-profile** command in global configuration mode. To attach an existing IPHC profile to an interface or subinterface, use the **iphc-profile** command in interface configuration mode. To delete the IPHC profile, use the **no** form of this command.

iphc-profile *profile-name* {**ietf** | **van-jacobson**}
no iphc-profile *profile-name*

Syntax Description

profile-name	Name of the IPHC profile to be created or attached. The IPHC profile name can be a maximum of 32 characters. The name may not include quotation marks, white space, or special characters.
ietf	Specifies that the IPHC profile is for Internet Engineering Task Force (IETF) header compression.
van-jacobson	Specifies that the IPHC profile is for Van Jacobson header compression.

Command Default

No IPHC profile is created or attached.

Command Modes

Global configuration (to create an IPHC profile) Interface configuration (to attach an existing IPHC profile to an interface or subinterface)

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

The **iphc-profile** command creates an IPHC profile used for enabling header compression and enters IPHC-profile configuration mode (config-iphcp). An IPHC profile is a template within which you can configure the type of header compression that you want to use, enable any optional features and settings for header compression, and then apply the profile to an interface, a subinterface, or a Frame Relay permanent virtual circuit (PVC).

Specifying the IPHC Profile Type

When you create an IPHC profile, you must specify the IPHC profile type by using either the **ietf** keyword or the **van-jacobson** keyword. The IETF profile type conforms to and supports the standards established with RFC 2507, RFC 2508, RFC 3544, and RFC 3545 and is typically associated with non-TCP header compression (for example, RTP header compression). The Van Jacobson profile type conforms to and supports the standards established with RFC 1144 and is typically associated with TCP header compression.

Note: If you are using Frame Relay encapsulation, you must specify the **ietf**keyword (not the **van-jacobson** keyword).

Considerations When Specifying the IPHC Profile Type

When specifying the IPHC profile type, consider whether you are compressing TCP traffic or non-TCP traffic (that is, RTP traffic). Also consider the header compression format capabilities of the remote network link that will receive traffic. The IPHC profile type that you specify directly affects the header compression format used on the remote network links to which the IPHC profile is applied. *Only* TCP traffic is compressed on remote network links using a Van Jacobson IPHC profile, whereas TCP *and/or* non-TCP traffic (for example, RTP traffic) is compressed on remote network links using an IETF IPHC profile.

Note The header compression format in use on the router that you are configuring and the header compression format in use on the remote network link must match.

Configurable Header Compression Features and Settings

The specific set of header compression features and settings that you can configure (that is, enable or modify) is determined by the IPHC profile type that you specify (either IETF or Van Jacobson) when you create the IPHC profile. Both sets are listed below.

If you specify Van Jacobson as the IPHC profile type, you can enable TCP header compression and set the number of TCP contexts. The table below lists each available Van Jacobson IPHC profile type header compression feature and setting and the command used to enable it.

Table 21: Van Jacobson IPHC Profile Type Header Compression Features and Settings

Command	Feature or Setting
tcp	Enables TCP header compression.
tcp contexts	Sets the number of contexts available for TCP header compression.

If you specify IETF as the IPHC profile type, you can enable non-TCP header compression (that is, RTP header compression), along with a number of additional features and settings. The table below lists each available IETF IPHC profile type header compression feature and setting and the command or commands used to enable it.

Table 22: IETF IPHC Profile Type Header Compression Features and Settings

Command	Feature or Setting
feedback	Enables the context-status feedback messages from the interface or link.
maximum header	Sets the maximum size of the compressed IP header.
non-tcp	Enables non-TCP header compression.
non-tcp contexts	Sets the number of contexts available for non-TCP header compression.
rtp	Enables RTP header compression.
recoverable-loss	Enables Enhanced Compressed Real-Time Transport Protocol (ECRTP) on an interface.
refresh max-period refresh max-time refresh rtp	Sets the context refresh (full-header refresh) options, such as the amount of time to wait before a full header is refreshed.

Command	Feature or Setting
tcp	Enables TCP header compression.
tcp contexts	Sets the number of contexts available for TCP header compression.

For More Information About IPHC Profiles

For more information about using IPHC profiles to configure header compression, see the "Header Compression" module and the "Configuring Header Compression Using IPHC Profiles" module of the Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.4T.

Examples

In the following example, an IPHC profile called profile1 is created, and the Van Jacobson IPHC profile type is specified.

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile1 van-jacobson
Router(config-iphcp)# end
```

In the following example, a second IPHC profile called profile2 is created. For this IPHC profile, the IETF IPHC profile type is specified.

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile2 ietf
Router(config-iphcp)# end
```

In the following example, an existing IPHC profile called profile2 is attached to serial interface 3/0. For this IPHC profile, the IPHC profile type (in this case, IETF) of profile2 is specified.

```
Router> enable
Router# configure terminal
Router(config)# interface serial 3/0
Router(config-if)# iphc-profile profile2 ietf
Router(config-iphcp)# end
```

Related Commands

Command	Description
feedback	Enables the context-status feedback messages from the interface or link.
maximum header	Specifies the maximum size of the compressed IP header.
non-tcp	Enables non-TCP header compression within an IPHC profile.
non-tcp contexts	Sets the number of contexts available for non-TCP header compression.
recoverable-loss	Enables ECRTP on an interface.
refresh max-period	Sets the number of packets sent between full-header refresh occurrences.
refresh max-time	Sets the amount of time to wait before a full-header refresh occurrence.
refresh rtp	Enables a context refresh occurrence for RTP header compression.

Command	Description
rtp	Enables RTP header compression within an IPHC profile.
show iphc-profile	Displays configuration information for one or more IPHC profiles.
tcp	Enables TCP header compression within an IPHC profile.
tcp contexts	Set the number of contexts available for TCP header compression.

keepalive

To enable keepalive packets and to specify the number of times that the Cisco IOS software tries to send keepalive packets without a response before bringing down the interface or before bringing down the tunnel protocol for a specific interface, use the **keepalive** command in interface configuration mode. When the keepalive function is enabled, a keepalive packet is sent at the specified time interval to keep the interface active. To turn off keepalive packets entirely, use the **no** form of this command.

keepalive [*period*[{**retries**}]]
no keepalive [*period*[{**proto-up**}]]

Syntax Description

period	(Optional) Integer value that represents the time interval, in seconds, between messages sent by the Cisco IOS software to ensure that a network interface is alive. • The valid range is from 0 to 32767 and the default value is 10.
retries	(Optional) Number of times that the device will continue to send keepalive packets without a response before bringing the interface down. • The valid range is 2 to 244. If omitted, the value that was previously set is used; if no value was specified, the default of 5 is used. • If this command is used with a tunnel interface, this argument value specifies the number of times that the device will continue to send keepalive packets without a response before bringing down the tunnel interface protocol.
proto-up	(Optional) Modifies the interface and protocol status to up even if the router is not connected to a wire or the interface of the peer router is down.

Command Default

The time interval between messages is10 seconds, and the number of retries is 3.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
12.2(8)T	This command was modified. The *retries* argument was added and made available on tunnel interfaces.
12.2(13)T	This command was modified. The default value for the *retries* argument was increased to 5.
12.2SX	This command was added in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(4)M8	This command was modified. The **proto-up** keyword was added.
15.2(2)SNI	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.
15.3(1)S	This command was integrated into Cisco IOS Release15.3(1)S.

Usage Guidelines

The **service interval**command must be enabled to run the **no keepalive**command.

Defaults for the keepalive Command

If you enter only the keepalive command with no arguments, default values for both arguments are used. If you enter the keepalive command and the timeout parameter, the default number of retries (5) is used. If you enter the **nokeepalive**command, keepalive packets are disabled on the interface. When the interface goes down, the session continues without shutting down because the keepalive packets are disabled.

Keepalive Time Interval

You can configure the keepalive time interval, which is the frequency at which the Cisco IOS software sends messages to itself (Ethernet and Token Ring) or to the other end (serial and tunnel), to ensure that a network interface is alive. The interval is adjustable in 1-second increments down to 1 second. An interface is declared down after five update intervals have passed without receiving a keepalive packet unless the retry value is set higher. If you are running a Cisco IOS image prior to Cisco IOS Release 12.2(13)T, the default retry value is 3.

Note Ethernet interface drivers on some access platforms use the keepalive time as the interval to test for network connectivity. By default, Ethernet link failure detection occurs between 1 and 9 seconds. Keepalive packets are still transmitted on the interface during this time.

Setting the keepalive timer to a low value is very useful for rapidly detecting Ethernet interface failures (transceiver cable disconnecting, cable not terminated, and so on).

Line Failure

A typical serial line failure involves losing the Carrier Detect (CD) signal. Because this sort of failure is typically noticed within a few milliseconds, adjusting the keepalive timer for quicker routing recovery is generally not useful.

Keepalive Packets with Tunnel Interfaces

Generic routing encapsulation (GRE) keepalive packets may be sent from both sides of a tunnel or from just one side. If they are sent from both sides, the period and retry parameters can be different at each side of the link. If you configure keepalives on only one side of the tunnel, the tunnel interface on the sending side might perceive the tunnel interface on the receiving side to be down because the sending interface is not receiving keepalives. From the receiving side of the tunnel, the link appears normal because no keepalives were enabled on the second side of the link.

Dropped Packets

Keepalive packets are treated as ordinary packets, so it is possible that they will be dropped. To reduce the chance that dropped keepalive packets will cause the tunnel interface to be taken down, increase the number of retries.

Note When adjusting the keepalive timer for a very low bandwidth serial interface, large datagrams can delay the smaller keepalive packets long enough to cause the line protocol to go down. You may need to experiment to determine the best values to use for the timeout and the number of retry attempts.

GRE Tunnels with IPsec

When GRE is used with IPsec, the keepalives are encrypted like any other traffic. As with user data packets, if the IKE and IPsec security associations are not already active on the GRE tunnel, the first GRE keepalive packet will trigger IKE/IPsec initialization.

Note GRE tunnel with IPSEC tunnel protection does not encrypt replies to incoming GRE keepalive packets. For more information, see the GRE Tunnel Keepalive Troubleshooting Technical Notes.

Examples

The following example shows how to enable keepalive packets and set the keepalive interval to 3 seconds:

```
Router(config)# interface ethernet 0
Router(config-if)# keepalive 3
```

The following example shows how to enable keepalive packets, set the keepalive interval to 3 seconds, and the retry value to 7 in a tunnel interface:

```
Router(config)# interface tunnel 1
Router(config-if)# keepalive 3 7
```

The following example shows how to bring up the interface of a router even if the peer router is down.

```
Router(config)# interface tunnel 1
Router(config)# service internal
Router(config-if)# no keepalive proto-up
```

Related Commands

Command	Description
service internal	Sets a primary or secondary IP address for an interface.

l2 vfi manual through loopback PA-MC-8TE1 + port adapter

l2 vfi manual

To create a Layer 2 virtual forwarding instance (VFI) and enter Layer 2 VFI manual configuration mode, use the **l2vfimanual** command in global configuration mode. To remove the Layer 2 VFI, use the **no** form of this command.

l2 vfi *name* **manual**
no l2 vfi *name* **manual**

Syntax Description

name	Name of a new or existing Layer 2 VFI .

Command Default

The Layer 2 VFI is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)SXF	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.0(1)M	This command was integrated into a release earlier than Cisco IOS Release 15.0(1)M.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.

Usage Guidelines

A VFI is a collection of data structures used by the data plane, software-based or hardware-based, to forward packets to one or more virtual circuits (VC). It is populated and updated by both the control plane and the data plane and also serves as the data structure interface between the control plane and the data plane.

Within the Layer 2 VFI manual configuration mode, you can configure the following parameters:

- VPN ID of a Virtual private LAN service (VPLS) domain
- Addresses of other PE routers in this domain
- Type of tunnel signaling and encapsulation mechanism for each peer

Within the Layer 2 VFI manual configuration mode, the following commands are available:

- **vpn id** *vpn-id*
- [**no**] **neighbor***remote-router-id* {**encapsulation** {**l2tpv3** | **mpls**} | **pw-class***pw-name*| **no-split-horizon**}

Examples

This example shows how to create a Layer 2 VFI, enter Layer 2 VFI manual configuration mode, and configure a VPN ID:

```
Router(config)# l2 vfi vfitest1 manual
Router(config-vfi)# vpn id 303
```

Related Commands

Command	Description
l2 vfi point-to-point	Establishes a point-to-point Layer 2 VFI between two separate networks.
vpn id	Configures a VPN ID in RFC 2685 format. You can change the value of the VPN ID only after its configuration, and you cannot remove it.
neighbor	Specifies the type of tunnel signaling and encapsulation mechanism for each peer.

l2protocol-tunnel

To enable the protocol tunneling on an interface and specify the type of protocol to be tunneled, use the **l2protocol-tunnel** command in global or interface configuration mode. To disable protocol tunneling, use the **no** form of this command.

Global Configuration
l2protocol-tunnel [{**cos** **cos-value** | **global** | **mac-address**}]
no l2protocol-tunnel

Interface Configuration
l2protocol-tunnel [{**cdp** | **lldp** | **stp** | **vtp**}]
no l2protocol-tunnel

Syntax Description

cos cos-value	(Optional) Specifies a class of service (CoS) value globally on all ingress Layer 2 protocol tunneling ports.
global	(Optional) Displays global settings.
mac-address	(Optional) Displays L2PT MAC address.
cdp	(Optional) Enables Cisco Discovery Protocol (CDP) tunneling.
lldp	(Optional) Enables Link Layer Discovery Protocol (LLDP) tunneling.
stp	(Optional) Enables Spanning Tree Protocol (STP) tunneling.
vtp	(Optional) Enables VLAN Trunking Protocol (VTP) tunneling.

Command Default

Disabled

Command Modes

Global configuration (config)

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.2(2)T	This command was modified. The **lldp**, cos, global, and mac-address keywords were added.

Usage Guidelines

On all the service provider edge switches, you must enable PortFast BPDU filtering on the 802.1Q tunnel ports by entering these commands:

```
Router(config-if)# spanning-tree bpdufilter enable
Router(config-if)# spanning-tree portfast
```

Note PortFast BPDU filtering is enabled automatically on tunnel ports.

If you do not specify a protocol, all protocols are tunneled.

You can configure protocol tunneling on VLAN and trunk interfaces.

You must enter the **switchport** command once without any keywords to configure the LAN port as a Layer 2 interface before you can enter additional **switchport** commands with keywords. This action is required only if you have not entered the **switchport** command for the interface.

Examples

This example shows how to enable a tunneling protocol on an interface:

```
Router> enable
Router# configure terminal
Router#(config)interface FastEthernet 0/0
Router(config-if)# l2protocol-tunnel cdp
```

This example shows how to disable a tunneling protocol on an interface:

```
Router> enable
Router# configure terminal
Router#(config)interface fastEthernet 4/0
Router(config-if)# no l2protocol-tunnel
Protocol tunneling disabled on interface fastEthernet 4/1
```

Related Commands

Command	Description
show l2protocol-tunnel	Displays the protocols that are tunneled on an interface or on all interfaces.
switchport	Modifies the switching characteristics of the Layer 2-switched interface.

l2protocol-tunnel cos

To specify a class of service (CoS) value globally on all ingress Layer-2 protocol tunneling ports, use the **l2protocol-tunnelcos**command in global configuration mode. To return to the default , use the **no** form of this command.

l2protocol-tunnel cos *cos-value*
no l2protocol-tunnel cos

Syntax Description

cos-value	CoS value; valid values are from 0 to 7.

Command Default

The *cos-value* is **5**

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The *cos-value* is the CoS value that you assign to the PDUs on a Layer 2-protocol tunnel port before tunneling the PDUs through the service-provider network.

You can specify a CoS value globally on all ingress Layer 2-protocol tunneling ports. Because the CoS value applies to all ingress tunneling ports, all encapsulated PDUs that are sent out by the Cisco 7600 series router have the same CoS value.

On all the service-provider edge switches, you must enable PortFast BPDU filtering on the 802.1Q tunnel ports by entering these commands:

```
Router(config-if)# spanning-tree bpdufilter enable
Router(config-if)# spanning-tree portfast
```

Note PortFast BPDU filtering is enabled automatically on tunnel ports.

Examples

This example shows how to specify a CoS value on all ingress Layer 2-protocol tunneling ports:

```
Router(config)# l2protocol-tunnel cos 6
Router(config)#
```

Related Commands

Command	Description
show l2protocol-tunnel	Displays the protocols that are tunneled on an interface or on all interfaces.

l2protocol-tunnel drop-threshold

To specify the maximum number of packets that can be processed for the specified protocol on that interface before being dropped, use the **l2protocol-tunneldrop-threshold** command in interface configuration mode. To reset all the threshold values to 0 and disable the drop threshold, use the **no** form of this command.

l2protocol-tunnel drop-threshold [{**cdp** | **stp** | **vtp**}] *packets*
no l2protocol-tunnel drop-threshold [{**cdp** | **stp** | **vtp**}]

Syntax Description

cdp	(Optional) Specifies CDP packets.
stp	(Optional) Specifies STP packets.
vtp	(Optional) Specifies VTP packets.
packets	Maximum number of packets; valid values are from 1 to 4096 packets.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

On all the service-provider edge switches, you must enable PortFast BPDU filtering on the 802.1Q tunnel ports by entering these commands:

```
Router(config-if)# spanning-tree bpdufilter enable
Router(config-if)# spanning-tree portfast
```

Note PortFast BPDU filtering is enabled automatically on tunnel ports.

If you do not specify a protocol, the threshold applies to all protocols.

You can configure protocol tunneling on switch ports only. You must enter the **switchport** command once without any keywords to configure the LAN port as a Layer 2 interface before you can enter additional **switchport** commands with keywords. This action is required only if you have not entered the **switchport** command for the interface.

Refer to the “Configuring IEEE 802.1Q Tunneling and Layer 2 Protocol Tunneling” chapter of the Cisco 7600 Series Router Cisco IOS Software Configuration Guide for additional information on setting the drop threshold value.

Examples

This example shows how to set the drop threshold:

```
Router(config-if)# switchport
Router(config-if)# l2protocol-tunnel drop-threshold 3000
Router(config-if)#
```

Related Commands

Command	Description
l2protocol-tunnel	Enables the protocol tunneling on an interface and specifies the type of protocol to be tunneled.
l2protocol-tunnel cos	Specifies a CoS value globally on all ingress Layer-2 protocol tunneling ports.
l2protocol-tunnel global drop-threshold	Enables rate limiting at the software level.
l2protocol-tunnel shutdown-threshold	Specifies the maximum number of packets that can be processed for the specified protocol on that interface in 1 second.
show l2protocol-tunnel	Displays the protocols that are tunneled on an interface or on all interfaces.
switchport	Modifies the switching characteristics of the Layer 2-switched interface.

l2protocol-tunnel global drop-threshold

To enable rate limiting at the software level, use the **l2protocol-tunnelglobaldrop-threshold** command in global configuration mode. To disable the software rate limiter on the Cisco 7600 series routers, use the **no** form of this command.

l2protocol-tunnel global drop-threshold *threshold*
no l2protocol-tunnel global drop-threshold

Syntax Description

threshold	Maximum rate of incoming PDUs before excessive PDUs are dropped; valid values are from 100 to 20000 PDUs.

Command Default

Global thresholds are not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.2(17a)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

All three PDUs (normal BPDU, CDP, and VTP packets) that arrive on Layer 2-protocol tunnel-enabled ports are rate limited. Rate limiting occurs in the ingress direction in Layer 2-protocol tunneling. If the rate of the incoming PDUs exceeds the configured threshold , the excessive PDUs are dropped.

Examples

This example shows how to enable rate limiting globally:

```
Router(config)# l2protocol-tunnel global drop-threshold 3000
Router(config)#
```

Related Commands

Command	Description
l2protocol-tunnel	Enables the protocol tunneling on an interface and specifies the type of protocol to be tunneled.
l2protocol-tunnel cos	Specifies a CoS value globally on all ingress Layer-2 protocol tunneling ports.
l2protocol-tunnel drop-threshold	Specifies the maximum number of packets that can be processed for the specified protocol on that interface before being dropped.
l2protocol-tunnel shutdown-threshold	Specifies the maximum number of packets that can be processed for the specified protocol on that interface in 1 second.
show l2protocol-tunnel	Displays the protocols that are tunneled on an interface or on all interfaces.

l2protocol-tunnel point-to-point

To enable point-to-point protocol tunneling, use the l2protocol-tunnel point-to-point command in interface configuration mode. To disable, use the **no** form of this command.

l2protocol-tunnel point-to-point [{**pagp** | **lacp** | **udld**}]
no l2protocol-tunnel point-to-point [{**pagp** | **lacp** | **udld**}]

Syntax Description

pagp	(Optional) Enables port aggregation on a point-to-point protocol tunneling.
lacp	(Optional) Enables link aggregation on a point-to-point protocol tunneling.
udld	(Optional) Enables a unidirectional link dectection on a point-to-point protocol tunneling.

Command Default

If no keyword is selected, tunneling is enabled for all three protocols.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

To avoid a network failure, make sure that the network is a point-to-point topology before you enable tunneling for PAgP, LACP, or UDLD packets.

Examples

The following example shows how to enable link aggregation on a point-to-point protocol tunneling:

```
Router(config-if
)# l2protocol-tunnel point-to-point lacp
```

Related Commands

Command	Description
show l2protocol-tunnel	Displays the enabled protocols and their values.

l2protocol-tunnel shutdown-threshold

To specify the maximum number of packets that can be processed for the specified protocol on that interface in 1 second, use the **l2protocol-tunnelshutdown-threshold**command in interface configuration mode. To reset all the threshold values to 0 and disable the shutdown threshold, use the **no** form ofthis command.

l2protocol-tunnel shutdown-threshold [{**cdp** | **stp** | **vtp**}] *packets*
no l2protocol-tunnel shutdown-threshold [{**cdp** | **stp** | **vtp**}] *packets*

Syntax Description

cdp	(Optional) Specifies CDP tunneling.
stp	(Optional) Specifies STP tunneling.
vtp	(Optional) Specifies VTP tunneling.
packets	Shutdown threshold; valid values are from 1 to 4096.

Command Default

This command has no default settings.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

When the number of *packets* is exceeded, the port is put in error-disabled state.

On all the service-provider edge switches, you must enable PortFast BPDU filtering on the 802.1Q tunnel ports by entering these commands:

```
Router(config-if)# spanning-tree bpdufilter enable
Router(config-if)# spanning-tree portfast
```

Note PortFast BPDU filtering is enabled automatically on tunnel ports.

If you do not specify a protocol, the *packets* value applies to all protocols.

You can configure protocol tunneling on switch ports only. You must enter the **switchport** command once without any keywords to configure the LAN port as a Layer 2 interface before you can enter additional **switchport** commands with keywords. This action is required only if you have not entered the **switchport** command for the interface.

Refer to the “Configuring IEEE 802.1Q Tunneling and Layer 2 Protocol Tunneling” chapter of the Cisco 7600 Series Router Cisco IOS Software Configuration Guide for additional information on setting the drop threshold value.

Examples

This example shows how to specify the maximum number of CDP packets that can be processed on that interface in 1 second:

```
Router(config-if)# switchport
Router(config-if)# l2protocol-tunnel shutdown-threshold cdp 200
Router(config-if)#
```

Related Commands

Command	Description
l2protocol-tunnel	Enables the protocol tunneling on an interface and specifies the type of protocol to be tunneled.
show l2protocol-tunnel	Displays the protocols that are tunneled on an interface or on all interfaces.
switchport	Modifies the switching characteristics of the Layer 2-switched interface.

l3vpn encapsulation ip

To configure an L3VPN encapsulation profile, use the **l3vpnencapsulationip** command in global configuration mode. To remove the encapsulation profile, use the **no** form of this command.

l3vpn encapsulation ip *profile name*
no l3vpn encapsulation ip *profile name*

Syntax Description

profile name	Name of the Layer 3 encapsulation profile.

Command Default

The L3VPN encapsulation profile is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.

Usage Guidelines

When you use the **l3vpnencapsulationip** command you enter into L3VPN encapsulation configuration mode. You can then specify the transport source mode and interface using the**transportipv4** command, set the GRE key using the **protocolgre** command, and configure the L3VPN encapsulation profile.

Examples

The following example shows how to configure an L3VPN encapsulation profile:

```
Router(config)# l3vpn encapsulation ip tunnelencap
```

Related Commands

Command	Description
show l3vpn encapsulation ip	Displays the profile health and the underlying tunnel interface.
transport ipv4	Specifies IPv4 transport source mode and the transport source interface.
protocol gre	Specifies GRE as the tunnel mode and sets the GRE key.

lacp active-port distribution automatic

To have an effective auto interleaved port priority distribution of active and bundled ports across different slots that are part of the same port channel distributed EtherChannel (DEC) and multichassis EtherChannel (MEC), use the **lacp active-port distribution automatic**command in port channel configuration mode.

lacp active-port distribution automatic
no lacp active-port distribution automatic

Syntax Description

This command has no keywords or arguments.

Command Default

Auto interleaved port priority is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI4	This command was introduced.

Usage Guidelines

The auto interleaved port-priority feature automatically distributes active and bundled ports based on the position of a port link when it comes up and is effective only if you configure it on the system that has the higher LACP system priority.

The port priority per port that you configured continues to take precedence over a dynamic port number. You need to perform a shutdown and no shutdown on the interface port channel to enable the auto interleaved port priority feature on all ports.

Examples

This example shows how to configure interleaved port priority:

```
Router(config)# interface port23
Router(config-if)# lacp active-port distribution automatic
Please shut/no shut the port-channel for configuration to take effect immediately.
Router(config-if)# shutdown
Router(config-if)# no shutdown
Router(config-if)# end
```

This example shows how to verify that interleaved port priority is configured:

```
Router# show running interface port23
Building configuration...
Current configuration : 81 bytes
!
interface Port-channel23
no switchport
no ip address
lacp max-bundle 4
lacp active-port distribution automatic
end
Router# show etherchannel 23 summary
Flags: D - down P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
```

```
U - in use N - not in use, no aggregation
f - failed to allocate aggregator
M - not in use, no aggregation due to minimum links not met
m - not in use, port not aggregated due to minimum links not met
u - unsuitable for bundling
d - default port
w - waiting to be aggregated
Number of channel-groups in use: 9
Number of aggregators: 9
Group     Port-channel Protocol      Ports
------+-------------+-----------+-----------------------------------------------
23      Po23(RU)       LACP       Gi1/1/21(P) Gi1/1/22(P) Gi1/1/23(P)
                                  Gi1/1/24(P) Gi2/1/17(H) Gi2/1/18(H)
                                  Gi2/1/19(H) Gi2/1/20(H)
Last applied Hash Distribution Algorithm: Fixed
```

Note The four active and bundled ports are from the same chassis and slot.

Related Commands

Command	Description
show etherchannel	Displays EtherChannel information for a port channel.

lacp fast-switchover

To enable Link Aggregation Control Protocol (LACP) 1:1 link redundancy, use the **lacp fast-switchover** command in interface configuration mode. To dis able LACP 1:1 link redundancy, use the **no** form of this command.

lacp fast-switchover
no lacp fast-switchover

Syntax Description

This command has no arguments or keywords.

Command Default

LACP 1:1 link redundancy is disabled by default.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	Support for this command was implemented on the Cisco 10000 series router and integrated into Cisco IOS Release 12.2(33)SB. The time allowed for a link switchover was modified from the default of 2 seconds to 250 milliseconds.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5

Usage Guidelines

Prior to entering the **lacp fast-switchover** command, you must ensure the following:

- The port channel protocol type is LACP.
- The **lacp max-bundle 1**command has been entered on the port channel. The **lacp fast-switchover** command will not affect the **lacp max-bundle** command.

When you enable LACP 1:1 link redundancy, based on the system priority and port priority, the port with the higher system priority chooses the link as the active link and the other link as the standby link. When the active link fails, the standby link is selected as the new active link without taking down the port channel. When the original active link recovers, it reverts to its active link status. During this change-over, the port channel is also up.

Note We recommend that you configure two ports only (one active and one hot-standby) in the bundle for optimum performance.

You can enter this command on any port channels with different EtherChannel protocol types of LACP, Port Aggregation Protocol (PAgP), or Fast EtherChannel (FEC).

Examples

This example shows how to enable LACP 1:1 link redundancy:

```
Router(config-if)# lacp fast-switchover
```

This example shows how to disable LACP 1:1 link redundancy:

```
Router(config-if)# no lacp fast-switchover
```

Related Commands

Command	Description
lacp max-bundle	Assigns and configures an EtherChannel interface to an EtherChannel group.
show etherchannel	Displays the EtherChannel information for a channel.

lacp max-bundle

To define the maximum number of active bundled Link Aggregation Control Protocol (LACP) ports allowed in a port channel, use the **lacp max-bundle** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

lacp max-bundle *max-bundles*
no lacp max-bundle

Syntax Description

max-bundles	Maximum number of active bundled ports allowed in the port channel. Valid values are from 1 to 8. On the Cisco ASR 1000 series router, valid values are 1 to 4. The default settings are as follows: • Maximum of 8 bundled ports per port channel. • Maximum of 8 bundled ports and 8 hot-standby ports per port channel if the port channels on both sides of the LACP bundle are configured in the same way. • On the Cisco 10000 series router, maximum of 8 bundled ports per port channel.

Command Default

A maximum number of active bundled ports is not configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	Support for this command was implemented on the Cisco 10000 series router and integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	Support for this command on the Cisco 7600 router was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	On the Cisco 10000 series router, the maximum number of bundled ports per port channel was increased from 4 to 8.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

The value specified in the *max-bundles* argument determines the number of active links that are bundled in the port channel. The remaining links are in hot-standby mode.

On the Cisco 10000 series router, this command requires a Performance Routing Engine 2 (PRE2) or PRE3.

Examples

This example shows how to set 3 ports to bundle in port channel 2:

```
Router(config)# interface port-channel 2
Router(config-if)# lacp max-bundle 3
Router(config-if)#
```

Related Commands

Command	Description
interface port-channel	Creates a port-channel virtual interface and puts the CLI in interface configuration mode.
ip address	Sets a primary or secondary IP address on an interface.
show etherchannel	Displays the EtherChannel information for a channel.
show interfaces port-channel	Displays traffic that is seen by a specific port channel.

lacp port-priority

To set the priority for a physical interface, use the **lacp port-priority** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

lacp port-priority *priority*

no lacp port-priority

Syntax Description

priority	Integer from 1 to 65535 that indicates the priority for the physical interface. The default is 32768. • On the Cisco ASR 1000 series router, the range is 0 to 65535.

Command Default

The default port priority is set.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1(13)EW	This command was introduced on the Cisco Catalyst 4500 series switches.
12.2(14)SX	Support for this command on the Supervisor Engine 720 was integrated into Cisco IOS Release12.2(14)SX.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was integrated into Cisco IOS Release12.2(17d) SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	Support for this command on the Cisco 7600 router was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

You may assign a port priority to each port on a device running Link Aggregation Control Protocol (LACP). You can specify the port priority by using the **lacp port-priority** command at the command-line interface (CLI) or use the default port priority (32768) that is carried as part of the LACP protocol data unit (PDU) exchanged with the partner. Port priority is used to decide which ports should be put in standby mode when a hardware limitation or the **lacp max-bundle** command configuration prevents all compatible ports from aggregating. Priority is supported only on port channels with LACP-enabled physical interfaces.

Note A high priority number means a low priority.

Port priority together with port number form a port identifier.

To verify the configured port priority, issue the **show lacp** command.

Examples

This example shows how to set a priority of 23700 for an interface:

```
Device> enable
Device#  configure terminal
Device(config)#  interface ethernet0/0
Device(config-if)# lacp port-priority 23700
Device(config-if)#
```

Related Commands

Command	Description
channel-group	Assigns and configures an EtherChannel interface to an EtherChannel group.
debug lacp	Enables debugging of LACP activities.
lacp max-bundle	Defines the maximum number of active bundled LACP ports allowed in a port channel.
lacp system-priority	Sets the priority of the system.
show lacp	Displays information about LACP activity on the device.

lacp rate

To set the rate at which Link Aggregation Control Protocol (LACP) control packets are ingressed to an LACP-supported interface, use the **lacp rate** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

lacp rate {**normal** | **fast**}
no lacp rate

Syntax Description

normal	Specifies that LACP control packets are ingressed at the normal rate, every 30 seconds after the link is bundled.
fast	Specifies that LACP control packets are ingressed at the fast rate, once every 1 second.

Command Default

The default ingressed rate for control packets is 30 seconds after the link is bundled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)SXF2	This command was introduced on the Catalyst 6500 series switch.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 3.6S	This command was implemented on Cisco ASR 1000 Series Aggregation Services Routers in Cisco IOS XE Release 3.6S.

Usage Guidelines

Use this command to modify the duration of a LACP timeout. The LACP timeout value is set on Cisco switches to a value of 90 seconds. Using the **lacp rate** command, you can select the LACP timeout value for a switch to be either 30 seconds or 1 second.

This command is supported only on LACP-enabled interfaces.

Examples

This example shows how to specify the fast (1-second) ingress rate on interface Ethernet 0/1:

```
Router(config)# interface ethernet 0/1
Router(config-if)# lacp rate fast
```

Related Commands

Command	Description
show lacp	Displays LACP information.

lacp system-priority

To set the priority for a system, use the **lacp system-priority** command in global configuration mode. To return to the default setting, use the **no** form of this command.

lacp system-priority *priority*

no lacp system-priority

Syntax Description

priority	Integer from 1 to 65535 that indicates the priority for the system. The default is 32768. • On the Cisco ASR 1000 series router, the range is 0 to 65535.

Command Default

The default system priority is set.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(13)EW	This command was introduced on the Cisco Catalyst 4500 series switches.
12.2(14)SX	Support for this command on the Supervisor Engine 720 was integrated into Cisco IOS Release12.2(14)SX.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was integrated into Cisco IOS Release12.2(17d) SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	Support for this command on the Cisco 7600 router was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

You can assign a system priority to each device running Link Aggregation Control Protocol (LACP). You can specify the system priority by using the **lacp system-priority** command at the command-line interface (CLI) or use the default system priority (32768) that is carried as part of the LACP protocol data unit (PDU) exchanged with the partner. System priority is used with the MAC address of the device to form the system ID and also is used during negotiation with other systems. Priority is supported only on port channels with LACP-enabled physical interfaces.

Note A high priority number means a low priority.

To verify the configured system priority, issue the **show lacp** command.

Examples

The following example shows how to set a system priority of 25500 for a device:

```
Router> enable
Router# configure terminal
Router(config)# lacp system-priority 25500
```

Related Commands

Command	Description
channel-group	Assigns and configures an EtherChannel interface to an EtherChannel group.
debug lacp	Enables debugging of LACP activities.
lacp port-priority	Sets the priority of a port.
show lacp	Displays information about LACP activity on the device.

lbo

To set a cable length longer than 655 feet for a DS-1 link, use the**lbo**command in interface configuration mode on the interface for a T1 link. To delete the **lbo**value, use the **no** form of this command.

lbo {**long** {**gain26** | **gain36**} {**-15db** | **-22 . 5db** | **-7 . 5db** | **0db**} | **short** {**133** | **266** | **399** | **533** | **655**}}
no lbo

Syntax Description

long	Specifies the long-haul mode where the gain and line build out must be configured.
gain26	Specifies the decibel pulse gain at 26 decibels. This is the default pulse gain.
gain36	Specifies the decibel pulse gain at 36 decibels.
-15db	Specifies the decibel pulse rate at -15 decibels.
-22.5db	Specifies the decibel pulse rate at -22.5 decibels.
-7.5db	Specifies the decibel pulse rate at -7.5 decibels.
0db	Specifies the decibel pulse rate at 0 decibels. This is the default.
short	Specifies the short-haul mode where the cable length, in feet, must be configured.
133	Specifies a cable length from 0 to 133 feet.
266	Specifies a cable length from 134 to 266 feet.
399	Specifies a cable length from 267 to 399 feet.
533	Specifies a cable length from 400 to 533 feet.
655	Specifies a cable length from 534 to 655 feet.

Command Default

gain26 and**0db**

Command Modes

Interface configuration

Command History

Release	Modification
11.3MA	This command was introduced as a Cisco MC3810 controller configuration command.
12.0(5)XE	The command was introduced as an ATM interface command.
12.0(7)XE1	This command was implemented on Cisco 7100 series routers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is supported on T1 links only.

Each T1 port can operate in long-haul or short-haul mode. In long haul mode, the user must specify the gain and the line build out. In short-haul mode, the user must specify the cable length in feet.

The transmit attenuation value is best obtained by experimentation. If the signal received by the far-end equipment is too strong, reduce the transmit level by entering additional attenuation.

Examples

On Cisco 7100 or Cisco 7200 series routers, the following example specifies a pulse gain of 36 decibels and a decibel pulse rate of -7.5 decibels:

```
Router(config)# interface atm 1/2
Router(config-if)# lbo long gain36 -7.5db
```

lex burned-in-address

To set the burned-in MAC address for a LAN Extender interface, use the **lexburned-in-address** command in interface configuration mode. To clear the burned-in MAC address, use the **no** form of this command.

lex burned-in-address *ieee-address*
no lex burned-in-addresslex burned-in-address command

Syntax Description

ieee-address	48-bit IEEE MAC address written as a dotted triplet of 4-digit hexadecimal numbers.

Command Default

No burned-in MAC address is set.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(15)T	This command is no longer supported in Cisco_IOS Mainline or Technology-based (T) releases. It may continue to appear in Cisco_IOS 12.2S-family releases.

Usage Guidelines

Use this command only on a LAN Extender interface that is not currently active (not bound to a serial interface).

Examples

The following example sets the burned-in MAC address on LAN Extender interface 0:

```
Router(config)# interface serial 4
Router(config-if)# encapsulation ppp
Router(config)# interface lex 0
Router(config-if)# lex burned-in-address 0000.0c00.0001
Router(config-if)  ip address 10.108.172.21 255.255.255.0
```

lex input-address-list

To assign an access list that filters on MAC addresses, use the **lexinput-address-list** command in interface configuration mode. To remove an access list from the interface, use the **no** form of this command.

lex input-address-list *access-list-number*
no lex input-address-listlex input-address-list command

Syntax Description

access-list-number	Number of the access list assigned with the **access-list** global configuration command. It can be a number from 700 to 799.

Command Default

No access lists are preassigned to a LAN Extender interface.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(15)T	This command is no longer supported in Cisco_IOS Mainline or Technology-based (T) releases. It may continue to appear in Cisco_IOS 12.2S-family releases.

Usage Guidelines

Use the **lexinput-address-list** command to filter the packets that are allowed to pass from the LAN Extender to the core router. The access list filters packets on the basis of the source MAC address.

The LAN Extender interface does not process MAC-address masks. Therefore, you should omit the mask from the **access-list** commands.

For LAN Extender interfaces, an implicit permit everything entry is automatically defined at the end of an access list. Note that this default differs from other access lists, which have an implicit deny everything entry at the end of each access list.

Examples

The following example applies access list 710 to LAN Extender interface 0. This access list denies all packets from MAC address 0800.0214.2776 and permits all other packets.

```
Router(config-if)# access-list 710 deny 0800.0214.2776
Router(config)# interface lex 0
Router(config-if)# lex input-address-list 710
```

Related Commands

Command	Description
access-list	Configures the access list mechanism for filtering frames by protocol type or vendor code.

lex input-type-list

To assign an access list that filters Ethernet packets by type code, use the **lexinput-type-list** command in interface configuration mode. To remove an access list from an interface, use the **no** form of this command.

lex input-type-list *access-list-number*
no lex input-type-list lex input-type-list command

Syntax Description

access-list-number	Number of the access list that you assigned with the **access-list** command. It can be a number in the range 200 to 299.

Command Default

No access lists are preassigned to a LAN Extender interface.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(15)T	This command is no longer supported in Cisco_IOS Mainline or Technology-based (T) releases. It may continue to appear in Cisco_IOS 12.2S-family releases.

Usage Guidelines

Filtering is done on the LAN Extender chassis.

The LAN Extender interface does not process masks. Therefore, you should omit the mask from the **access-list** commands.

For LAN Extender interfaces, an implicit permit everything entry is automatically defined at the end of an access list. Note that this default differs from other access lists, which have an implicit deny everything entry at the end of each access list.

Examples

The following example applies access list 220 to LAN Extender interface 0. This access list denies all AppleTalk packets (packets with a type field of 0x809B) and permits all other packets.

```
Router(config-if)# access-list 220 deny 0x809B 0x0000
Router(config)# interface lex 0
Router(config-if)# lex input-type-list 220
```

Related Commands

Command	Description
access-list	Configures the access list mechanism for filtering frames by protocol type or vendor code.

lex priority-group

To activate priority output queueing on the LAN Extender, use the **lexpriority-group** command in interface configuration mode. To disable priority output queueing, use the **no** form of this command.

lex priority-group *group*
no lex priority-group

Syntax Description

group	Number of the priority group. It can be a number in the range 1 to 10.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(15)T	This command is no longer supported in Cisco_IOS Mainline or Technology-based (T) releases. It may continue to appear in Cisco_IOS 12.2S-family releases.

Usage Guidelines

To define queueing priorities, use the **priority-listprotocol** global configuration command. Note that you can use only the following forms of this command:

```
priority-list

list
 protocol

protocol

{
high
 |
medium
 |
normal
 |
low
priority-list

list
 protocol
 bridge

{
high
 |
medium
 |
normal
 |
low
}
```

list

list-number

If you specify a protocol that does not have an assigned Ethernet type code, such as **x25**, **stun**, or **pad**, it is ignored and will not participate in priority output queueing.

Examples

The following example activates priority output queueing on LAN Extender interface 0:

```
Router(config-if)# priority-list 5 protocol bridge medium list 701
Router(config-if)# lex interface 0
Router(config-if)# lex priority-group 5
```

Related Commands

Command	Description
priority-list protocol	Establishes queueing priorities based on the protocol type.

lex retry-count

To define the number of times to resend commands to the LAN Extender chassis, use the **lexretry-count** command in interface configuration mode. To return to the default value, use the **no** form of this command.

lex retry-count *number*
no lex retry-count *number* **lex retry-count command**

Syntax Description

number	Number of times to retry sending commands to the LAN Extender. It can be a number in the range 0 to 100. The default is 10.

Command Default

10 retries

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(15)T	This command is no longer supported in Cisco_IOS Mainline or Technology-based (T) releases. It may continue to appear in Cisco_IOS 12.2S-family releases.

Usage Guidelines

After the router has sent a command the specified number of times without receiving an acknowledgment from the LAN Extender, it stops sending the command altogether.

Examples

The following example resends commands 20 times to the LAN Extender:

```
Router(config-if)# lex interface 0
Router(config-if)# lex retry-count 20
```

Related Commands

Command	Description
lex timeout	Defines the amount of time to wait for a response from the LAN Extender.

lex timeout

To define the amount of time to wait for a response from the LAN Extender, use the **lextimeout** command in interface configuration mode. To return to the default time, use the **no** form of this command.

lex timeout *milliseconds*
no lex timeout [*milliseconds*] **lex timeout command**

Syntax Description

milliseconds	Time, in milliseconds, to wait for a response from the LAN Extender before resending the command. It can be a number in the range 500 to 60,000. The default is 2000 ms.

Command Default

2000 ms (2 seconds)

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(15)T	This command is no longer supported in Cisco_IOS Mainline or Technology-based (T) releases. It may continue to appear in Cisco_IOS 12.2S-family releases.

Usage Guidelines

The **lextimeout** command defines the amount of time that the router waits to receive an acknowledgment after having sent a command to the LAN Extender.

Examples

The following example causes unacknowledged packets to be resent at 4-second intervals:

```
Router(config-if)# lex interface 0
Router(config-if)# lex timeout 4000
```

Related Commands

Command	Description
lex retry-count	Defines the number of times to resend commands to the LAN Extender chassis.

license feature gnss

To configure the license for the global navigation satellite system (GNSS) module on the Cisco ASR 920 routers, use the **license feature gnss** command in the global configuration mode. To remove the license, use the **no** form of this command.

license feature gnss
no license feature gnss

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
IOS-XE 3.17	This command was introduced on the Cisco ASR 920 routers.

Usage Guidelines

Only when the GNSS license is in use, the **shutdown** and **no shutdown** operations for the GNSS module can be performed.

Examples

The following example shows how to configure the GNSS license:

```
Router# configure terminal
Router(config)# license feature gnss
```

Related Commands

Command	Description
gnss	Configures the GNSS on the router.

linecard-group y-cable

To create a line card group for one-to-one line card redundancy, use the linecard-group y-cable command in redundancy mode. To remove the line card redundancy group, use the no form of this command.

linecard-group *linecard-groupId* **y-cable**
no linecard-group *linecard-groupId* **y-cable**

Syntax Description

linecard-groupId	An unsigned integer in the range 0 to the (maximum number of chassis line card subslots/2) -1.
y-cable	The link protection type for the line card group.

Command Default

No default behavior or values .

Command Modes

Redundancy

Command History

Release	Modification
12.2(28)SB	This command was introduced on the Cisco 10000 series router.

Usage Guidelines

The no linecard-group y-cable command removes the line card redundancy group and frees the *linecard-groupId*for reuse. The no linecard-group y-cable command succeeds only if there are no subslot members in the line card redundancy group.

Examples

The following example creates line card group number 1 for one-to-one line card redundancy:

```
Router(config)# redundancy
Router(config-red)# linecard-group 1 y-cable
```

Related Commands

Command	Description
member subslot	Configures the redundancy role of a line card in the line card group.
redundancy	Enters redundancy mode.
show redundancy linecard	Displays information about a redundant line card or line card group.

linecode

To select the line-code type for T1 or E1 lines, use the **linecode** command in controller configuration mode.

linecode {**ami** | **b8zs** | **hdb3**}

Syntax Description

ami	Specifies alternate mark inversion (AMI) as the line-code type. Valid for T1 or E1 controllers. This is the default for T1 lines.
b8zs	Specifies B8ZS as the line-code type. Valid for T1 controller only.
hdb3	Specifies high-density bipolar 3 (hdb3) as the line-code type. Valid for E1 controller only. This is the default for E1 lines.

Command Default

AMI is the default for T1 lines. High-density bipolar 3 is the default for E1 lines.

Command Modes

Controller configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
XE 3.18SP	This command was integrated into Cisco NCS 4200 Series.
XE Everest 16.5.1	This command was integrated into Cisco NCS 4200 Series and Cisco ASR 900 Series Routers.

Usage Guidelines

Use this command in configurations in which the router or access server must communicate with T1 fractional data lines. The T1 service provider determines which line-code type, either **ami** or **b8zs**, is required for your T1 circuit. Likewise, the E1 service provider determines which line-code type, either **ami** or **hdb3**, is required for your E1 circuit.

This command does not have a **no** form.

Examples

The following example specifies B8ZS as the line-code type:

```
Router(config-controller)# linecode b8zs
```

line-mode

To configure the mode of the controller for the Symmetrical High-Speed Digital Subscriber Line (SHDSL) port, use the **line-mode** command in controller configuration mode. To return to the default two-wire mode, use the **no** form of this command.

line-mode [{**2-wire** | **4-wire** [{**enhanced** | **standard**}] | **auto**}]
no line-mode

Syntax Description

2-wire	(Optional) Configures the controller to operate in two-wire mode.
4-wire	(Optional) Configures the controller to operate in four-wire mode.
enhanced	(Optional) Configures 4-wire mode to exchange handshake status on both wire pairs. This is the default if the handshake mode is not specified.
standard	(Optional) Configures 4-wire mode to exchange handshake status on the master wire pair only.
auto	(Optional) Configures the controller to automatically operate in the mode to match the other line termination. This mode is compatible with a remote host that is in one of the following modes: • line-mode 2-wire line 0 • line-mode 2-wire line 1 • line-mode 4-wire enhanced

Command Default

The default is two-wire mode if this command is omitted or if the **4-wire** keyword is omitted.

Command Modes

Controller configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced on Cisco 2600 series and Cisco 3700 series routers.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T on Cisco 2600 series and Cisco 3700 series routers.
12.3(11)T	This command was implemented on Cisco 2800 and Cisco 3800 series routers.
12.3(14)T	This command was implemented on Cisco 1800 series routers.
12.4(2)XA	The **enhanced** and **standard** keywords were added to four-wire mode.
12.4(5)A	Modified **auto** keyword to to disallow use of **line-rate** command
12.4(4)T	Modified **auto** keyword to to disallow use of **line-rate** command

Usage Guidelines

This command is used to configure the controller for two-wire or four-wire mode.

Note To operate in four-wire mode for SHDSL, the **line-mode4-wire**command must be set.

Note When the **line-mode** command is set to **auto**, the **line-rate** command is not available.

Examples

4-Wire Line Mode Example

The following example shows how to configure the controller mode of DSL on the controller in slot 4 and port 0 to operate in four-wire mode:

```
Router(config)# controller dsl 4/0
Router(config-controller)# line-mode
 4-wire
```

CPE Line Mode Example

The following example configures the controller in slot 1 and port 0. The router is set to terminate as CPE with the line mode automatically selecting between two-wire mode and four-wire mode.

```
Router(config)# controller dsl 1/0
Router(config-controller)# line-mode auto
Router(config-controller)# line-term cpe
```

Related Commands

Command	Description
line-rate	Specifies a line rate for the DSL controller.
line-term	Specifies a termination for a line.

line-mode bonding

To enable bonding mode on a CPE, use the **line-mode bonding** command in controller configuration mode. To disable the bonding mode, use the **no** form of this command.

line-mode bonding
no line-mode bonding

Syntax Description

This command has no keywords or arguments.

Command Default

Bonding is not the default mode.

Command Modes

Controller configuration (config-controller)#

Command History

Release	Modification
15.4(4)T	This command was introduced.

Usage Guidelines

Use this command when a CPE is expected to operate in bonding mode.

Examples

The following example shows how to enable bonding mode:

```
Router(config-controller)# line-mode bonding
```

The following example shows how to disable bonding mode:

```
Router(config-controller)# no line-mode bonding
```

Related Commands

Command	Description
line-mode single-wire line	Enables single-wire (nonbonding) mode on a selected line.

line-mode single-wire line

To enable single-wire (nonbonding) mode on a selected line, use the **line-mode single-wire line** command in controller configuration mode. To disable the mode, use the **no** form of this command.

line-mode single-wire line *line-number*
`or`
line-mode single-wire line *line-number* **[profile 30a]**
no line-mode single-wire line *line-number*

Syntax Description

line-number	Line number. Valid values are either 1 or 0.
profile 30a	Enables 30a profile on line 1. If profile 30a is not specified, profiles 8a to 17a are enabled on that line.

Command Default

By default, single-wire mode is enabled on line 0 with profiles from 8a to17a enabled.

Command Modes

Controller configuration (config-controller)#

Command History

Release	Modification
15.4(4)T	This command was introduced.

Usage Guidelines

Use this command to configure either line 0 or line 1 in single-wire (non-bonding) mode.

Examples

The following example shows how to enable 30a profile on line 1:

```
Router(config-controller)# line-mode single-wire line 1 profile 30a
```

Related Commands

Command	Description
line-mode bonding	Changes the mode of a CPE to bonding.

line-rate

To specify a line rate for the DSL controller, use the **line-rate** command in controller configuration mode.

line-rate {**auto***rate*}

Syntax Description

auto	Allows the controller to select the rate. This option is available only in two-wire mode.
rate	DSL line rate, in kbps. The line will train at the selected rate plus 8 kbps of DSL framing overhead. The supported line rates are as follows: • For two-wire mode: • 192, 256, 320, 384, 448, 512, 576, 640, 704, 768, 832, 896, 960, 1024, 1088, 1152, 1216, 1280, 1344, 1408, 1472, 1536, 1600, 1664, 1728, 1792, 1856, 1920, 1984, 2048, 2112, 2176, 2240, and 2304 • For four-wire mode: • 384, 512, 640, 768, 896, 1024, 1152, 1280, 1408, 1536, 1664, 1792, 1920, 2048, 2176, 2304, 2432, 2560, 2688, 2816, 2944, 3072, 3200, 3328, 3456, 3584, 3712, 3840, 3968, 4096, 4224, 4352, 4480, and 4608

Command Default

No default behavior or values.

Command Modes

Controller configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced on Cisco 2600 series and Cisco 3700 series routers.
12.3(4)XG	This command was implemented on Cisco 1700 series routers.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T on Cisco 2600 series and Cisco 3700 series routers.
12.(11)T	This command was implemented on Cisco 2800 and Cisco 3800 series routers.
12.3(14)T	This command was implemented on Cisco 1800 series routers.
12.4(5)A	Modified **line-rate** command to be disallowed when **line-mode**command is set to **auto**.
12.4(4)T	Modified **line-rate** command to be disallowed when **line-mode**command is set to **auto**.

Usage Guidelines

This command does not have a **no** form.

This command specifies the DSL line rate for the Symmetrical High-Speed Digital Subscriber Line (SHDSL) port. Use this command to configure the line rate in two-wire or four-wire mode. The SHDSL rate is in kbps, but the line trains at the selected rate plus two times the 8 kbps of DSL framing overhead.

Note Automatic rate mode (auto) is used only in two-wire mode. It is not available in four-wire mode.

Note If different DSL line rates are configured at opposite ends of the DSL uplink, the actual DSL line rate is always the lower rate.

Note The maximum peak cell rate is 8 kbps less than the line rate.

Note When the **line-mode** command is set to **auto**, the **line-rate** command is not available.

Examples

The following example displays the **line-mode** command selecting four-wire mode, which is different from the previous line mode of the router as indicated by the router output, and then the line rate is selected. The rate of 4608 is selected, and the output of the router is shown.

```
Router(config)# controller dsl 1/0
Router(config-controller)# line-mode
 4-wire
Router(config-controller)#
*Jun 15 18:00:48.159: %CONTROLLER-5-UPDOWN: Controller DSL 1/0, changed state tn
*Jun 15 18:00:50.159: %LINK-3-UPDOWN: Interface ATM1/0, changed state to down
*Jun 15 18:00:51.159: %LINEPROTO-5-UPDOWN: Line protocol on Interface ATM1/0, cn
Router(config-controller)# line-rate
 4608
Router(config-controller)#
*Jun 15 18:01:36.627: %CONTROLLER-5-UPDOWN: Controller DSL 1/0, changed state tn
*Jun 15 18:01:36.967: %CONTROLLER-5-UPDOWN: Controller DSL 1/0, changed state tn
Router(config-controller)# exit
```

Related Commands

Command	Description
line-mode	Configures the mode of the controller.
line-term	Specifies a termination for a line.

line-term

To specify a termination for a line, use the **line-term** command in controller configuration mode.

line-term {**co** | **cpe**}

Syntax Description

co	Central office.
cpe	Customer premises equipment. This is the default.

Command Default

The default value is **cpe**.

Command Modes

Controller configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced on Cisco 2600 series and Cisco 3700 series routers.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T on Cisco 2600 series and Cisco 3700 series routers.
12.3(11)T	This command was implemented on Cisco 2800 and Cisco 3800 series routers.
12.3(14)T	This command was implemented on Cisco 1800 series routers.

Usage Guidelines

This command does not have a no form.

This command is used to configure the line termination for use as either the central office (CO) or the customer premises equipment (CPE).

Examples

The following example shows how to configure the controller in slot 1 and port 0. The router is set to terminate as CPE with the line mode automatically selecting between two-wire mode and four-wire mode.

```
Router(config)# controller dsl 1/0
Router(config-controller)# line-term
 cpe
Router(config-controller)# line-mode
auto

No change in line mode
```

Related Commands

Command	Description
line-mode	Configures the mode of the controller.
line-rate	Specifies a line rate for the DSL controller.

line-termination

To set the line termination on an E1 controller, use the **line-termination**command in controller configuration mode. To return to the default line termination, use the **no** form of this command.

line-termination {**75-ohm** | **120-ohm**}
no line-termination

Syntax Description

75-ohm	Specifies 75-ohm unbalanced termination.
120-ohm	Specifies 120-ohm balanced termination. This is the default.

Command Default

120-ohms

Command Modes

Controller configuration

Command History

Release	Modification
11.3(2)AA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command applies only to E1 controllers. To determine the line termination setting for the controller, use the **showcontrollerse1**command.

Examples

In the following example, the line termination is set to 75 ohms for the E1 port located in shelf 6, slot 0, port 0:

```
Router# configure terminal
Router(config)# controller e1 6/0/0
Router(config-controller)# line-termination 75-ohm
Router(config-controller)# end
```

Related Commands

Command	Description
show controllers e1	Displays information about the E1 links supported by the NPM (Cisco 4000) or MIP (Cisco 7500 series).

link debounce

To enable the debounce timer on an interface, use the **linkdebounce** command in interface configuration mode. To disable the timer, use the **no** form of this command.

link debounce [**time** *time*]
no link debounce

Syntax Description

time *time*	(Optional) Specifies the extended debounce timer; va lid values are from 100 to 5000 milliseconds.

Command Default

The table below lists the debounce timer defaults.

Table 23: Port Debounce Timer Delay Time

Port Type	Debounce Timer Disabled	Debounce Timer Enabled
10BASE-FL ports	300 milliseconds	3100 milliseconds
10/100BASE-TX ports	300 milliseconds	3100 milliseconds
100BASE-FX ports	300 milliseconds	3100 milliseconds
10/100/1000BASE-TX ports	300 milliseconds	3100 milliseconds
1000BASE-TX ports	300 milliseconds	3100 milliseconds
Fiber Gigabit ports	10 milliseconds	100 milliseconds
10-Gigabit ports except WS-X6501-10GEX4 and WS-X6502-10GE	10 milliseconds	100 milliseconds
WS-X6501-10GEX4 and WS-X6502-10GE 10-Gigabit ports	1000 milliseconds	3100 milliseconds

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX	This command was changed to remove support for the following modules: • WS-X6501-10GEX4 • WS-X6502-10GE
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **time***time* keyword and argument are supported on Gigabit Ethernet and 10-Gigabit Ethernet interfaces only.

The **linkdebounce** command is not supported on the following modules in releases prior to Release 2.2(17a)SX:

- WS-X6501-10GEX4
- WS-X6502-10GE

The debounce timer sets the amount of time that the firmware waits before it notifies the software that the link is down. The debounce timer does not apply to linkup because the linkup is immediately notified by the firmware.

The default debounce time applies when you enter the **linkdebounce** command with no arguments. For example, when you enter the **linkdebouncetime100** command, it is equivalent to entering the **linkdebounce** command with no arguments and you will see the following link debounce entry in the configuration:

```
interface GigabitEthernet1/1
 no ip address
 link debounce
```

Enter the **showinterfacesdebounce** command to display the debounce configuration of an interface.

Examples

This example shows how to configure the debounce timer on a Gigabit Ethernet fiber interface:

```
Router(config-if)# link debounce time 100
Router(config-if)#
```

Related Commands

Command	Description
show interfaces debounce	Displays the status and configuration for the debounce timer.

link state group

To configure the link state group, use the **linkstategroup** command in interface configuration mode.

link state group [*number*] {**upstream** | **downstream**}

Syntax Description

number	Specifies a link-state group. The acceptable range of group number is between 1 to 10 and the default value is 1.
upstream	Configures the interface as an upstream interface in the group.
downstream	Configures the interface as a downstream interface in the group.

Command Default

The default **linkstategroup**number is 1.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(1)S	This command was introduced.

Usage Guidelines

Link State Ttracking (LST), also known as trunk failover, is a feature that binds the link state of multiple interfaces. When you configure LST for the first time, add upstream interfaces to the link state group before adding the downstream interface, otherwise the downstream interfaces would move into error-disable mode. The maximum number of link state groups configurable is 10. These are the limitations:

- An interface can only be an upstream or downstream interface.
- An interface cannot be part of more than one link state tracking group.

Examples

The following example shows how to configure the link state group number.

```
Router# configure terminal
Router(config)# link state track 1
Router(config)# interface gigabitethernet3/1
Router(config-if)# link state group 1 upstream
Router(config-if)# interface gigabitethernet3/3
Router(config-if)# link state group 1 upstream
Router(config-if)# interface gigabitethernet3/5
Router(config-if)# link state group 1 downstream
Router(config-if)# interface gigabitethernet3/7
Router(config-if)# link state group 1 downstream
```

Related Commands

Command	Description
link state track	Configures the link-state track number.
show link state group	Displays the link-state group information.

link state track

To configure a link state tracking number, use the **linkstatetrack** command in global configuration mode. To restore the default **linkstatetrack**number, use the no form of this command.

link state track *number*
no link state track *number*

Syntax Description

number	Specifies the link state tracking number. The acceptable range is between 1 and 10 and the default value is 1.

Command Default

The default link state track number is 1.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)S	This command was introduced.

Usage Guidelines

Link State Ttracking (LST), also known as trunk failover, is a feature that binds the link state of multiple interfaces. When you configure LST for the first time, add upstream interfaces to the link state group before adding the downstream interface, otherwise the downstream interfaces would move into error-disable mode.

Examples

The following example shows how to configure the link state tracking number.

```
Router# configure terminal
Router(config)# link state track 1
```

Related Commands

Command	Description
link state group	Configures the link state group and the interface as either an upstream or downstream interface in the group.
show link state group	Displays the link state group information.

li-slot rp rate

To apply the user specified Packets Per Second (PPS) value when an Lawful Intercept (LI) is provisioned in RP mode, use the **li-slot rp rate** command in global configuration mode. To disable the user specified value, use the no form of this command .

li-slot rp rate *pps*

Syntax Description

pps	Packets per second (pps). The range is from 10 to 8500 for SUP720, 10 to 6000 for SUP32, and 10 to 12000 for RSP720.

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)S5	This command was introduced on the Cisco 7600 series routers.

Examples

This example shows how to apply PPS value when an LI is provisioned in RP mode:

```
router# configure terminal
router(config)# li-slot rp rate 5000
```

Related Commands

Command	Description
show mls rate-limit	Displays information about the configured rate limiters.

link-test

To reenable the link-test function on a port on an Ethernet hub of a Cisco 2505 or Cisco 2507 router, use the **link-test** command in hub configuration mode. To disable this function, use the **no** form of this command.

link-test commandlink-test
no link-test

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Hub configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command applies to a port on an Ethernet hub only. Disable this feature if a 10Base-T twisted-pair device at the other end of the hub does not implement the link test function.

Examples

The following example disables the link test function on hub 0, ports 1 through 3:

```
Router(config)#
 hub ethernet 0 1 3
Router(config-hub)#
 no link-test
```

Related Commands

Command	Description
hub	Enables and configures a port on an Ethernet hub of a Cisco 2505 or Cisco 2507 router.

load-balancing

To apply a load-balancing method to a Gigabit EtherChannel (GEC) interface, use the **load-balancing** command in interface configuration mode. To reset to the default, use the **no** form of this command.

load-balancing {**flow** | **vlan**}
no load-balancing

Syntax Description

flow	Flow-based load balancing is used.
vlan	VLAN-manual load balancing is used.

Command Default

The port channel uses the global load-balancing configuration.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 2.5	This command was introduced.

Usage Guidelines

The **load-balancing** command sets the load-balancing method on a specific port channel. The load-balancing method configured with this command takes precedence over the global configuration defined with the **port-channelload-balancingvlan-manual** command.

If you do not explicitly configure load balancing either globally or on the port channel, the load-balancing method on the port channel is set to flow-based.

Load balancing uses the concept of buckets to map traffic flows to the member links of the port channel. The different traffic flows are mapped to the buckets and each bucket has one active member link associated with it. All flows that are mapped to a bucket use the member link associated with that bucket.

There are two methods of load balancing on a GEC interface:

- VLAN-manual--All packets forwarded over the same VLAN subinterface are considered part of the same flow and are mapped to the member link specified in the configuration.
- Flow-based--Traffic flows are mapped to different member links based on the packet header.

Examples

This example shows how to set the load-balancing method to VLAN-manual:

```
Router(config)# interface port-channel 1
Router(config-if)# load-balancing vlan
```

Related Commands

Command	Description
interface port-channel	Creates a port-channel virtual interface.
port-channel load-balancing vlan-manual	Applies the VLAN-manual load-balancing method globally to all GEC interfaces.

Command	Description
show interfaces port-channel etherchannel	Displays the load-balancing bucket distribution currently in use for a GEC interface.
show etherchannel load-balancing	Displays the load-balancing method applied to GEC interfaces.

load-interval

To change the length of time for which data is used to compute load statistics, use the **load-interval** command in interface configuration, Frame Relay DLCI configuration, or template configuration modes. To revert to the default setting, use the **no**form of this command.

load-interval *seconds*
no **load-interval** *seconds*

Syntax Description

seconds	Length of time for which data is used to compute load statistics. Value is a multiple of 30, from 30 to 600 (30, 60, 90, 120, and so on). The default is 300 seconds.

Command Default

Enabled

Command Modes

Interface configuration

Frame Relay DLCI configuration

Template configuration (config-template)

Command History

Release	Modification
10.3	This command was introduced.
12.2(4)T	This command was made available in Frame Relay DLCI configuration mode.
12.2(18)SXF	Support for this command was introduced on the Supervisor Engine 720.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.
15.2(2)E	This command was integrated into Cisco IOS Release 15.2(2)E. This command is supported in template configuration mode.
Cisco IOS XE Release 3.6E	This command was integrated into Cisco IOS XE Release 3.6E. This command is supported in template configuration mode.

Usage Guidelines

To make computations more reactive to short bursts of traffic, you can shorten the length of time over which load averages are computed.

If the load interval is set to 30 seconds, new data is used for load calculations over a 30-second period. This data is used to compute load statistics, including the input rate in bits and packets per second, the output rate in bits and packets per second, the load, and reliability.

Load data is gathered every five seconds. This data is used for a weighted-average calculation in which recent load data has more weight in the computation than older load data. If the load interval is set to 30 seconds, the average is computed for the last 30 seconds of load data.

If you change the calculation interval from the default of five minutes to a shorter period of time, the input and output statistics that are displayed by the **show interface** command or the **show frame-relay pvc** command will be more current and will be based on more nearly instantaneous data, rather than reflecting the average load over a longer period of time.

This command is often used for dial backup purposes to increase or decrease the likelihood of implementation of a backup interface, but it can be used on any interface.

Examples

Interface Example

In the following example, the default average of five minutes is changed to a 30-second average. A burst in traffic that would not trigger a dial backup for an interface configured with the default five-minute interval might trigger a dial backup for this interface, which is set for the shorter 30-second interval.

```
Router(config)# interface serial 0
Router(config-if)# load-interval 30
```

Frame Relay PVC Example

In the following example, the load interval is set to 60 seconds for a Frame Relay PVC with the DLCI 100:

```
Router(config)# interface serial 1/1
Router(config-if)# frame-relay interface-dlci 100
Router(config-fr-dlci)# load-interval 60
```

Interface Template Example

In the following example, the load interval is set to 60 seconds in an interface template:

```
Device# configure terminal
Device(config)# template user-template1
Device(config-template)# load-interval 60
Device(config-template)# end
```

Related Commands

Command	Description
show interfaces	Displays statistics for all interfaces configured on the router or access server.

local ip address

To define an IP address to identify a local circuit emulation (CEM) channel, use the **localipaddress**command in CEM xconnect configuration mode.

local ip address *ip-address*

Syntax Description

ip-address	IP address of a regular or loopback interface in the local router. Default is 0.0.0.0

Command Default

The default local IP address is 0.0.0.0 for a CEM channel.

Command Modes

CEM xconnect configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

This command does not have a **no** form. To remove a local IP address, either configure a new local IP address or enter the **noxconnect** command to disable the connection and all its parameters.

The local IP address used to identify the local end of a CEM connection must be the same as the IP address defined by the *remote-ip-address*argument used in the **xconnect** command to identify the CEM channel at the other end of the CEM connection.

Note If there are multiple CEM connections that originate from the same router, they may share the same local IP address provided that each local IP address defines a unique UDP port number using the**localudpport** command.

Examples

The following example demonstrates how to configure the IP address of the local endpoint of the CEM over IP (CEoIP) connection.

```
Router(config-cem-xconnect)# local ip address 10.0.5.1
```

Related Commands

Command	Description
clear cem	Clears CEM statistics.
local udp port	Defines the UDP port at the local end of a CEM connection.
show cem	Displays CEM statistics.
xconnect (CEM)	Builds one end of a CEM connection and enters CEM xconnect configuration mode.

local-priority

To set the PTP clock's local priority.

Note This command is used only for the G.8275.1 telecom profile.

local-priority *local-priority*

Syntax Description

local-priority	Local priority value of the clock. The valid values are from 1 to 255.

Command Default

The default local priority is 1.

Command Modes

PTP Clock Configuration

Command History

Release	Modification
IOS-XE 3.18	This command was introduced.

Usage Guidelines

The configured local priority is ignored on ports without the G.8275.1 or G.8275.2 profile.

Examples

The following example demonstrates how to configure the local priority of the master-only ordinary clock.

```
Router# configure terminal
Router(config)# ptp clock ordinary domain 24
Router(config-ptp-clk)# local-priority 1
```

Related Commands

Command	Description
ptp clock	Creates a Precision Time Protocol clock and specifies the clock mode .
priority1	Sets priority1.
priority2	Sets priority2.
show ptp clock dataset default	Verifies the local priority of the PTP clock.

local udp port

To define the User Datagram Protocol (UDP) port of the local endpoint of a circuit emulation (CEM) connection, use the **localudpport**command in CEM xconnect configuration mode.

local udp port *port*

Syntax Description

port	Number of the CEM local UDP port. Possible values are 0, 2141, and 15872 through 16383. The default is 0.

Command Default

The default local UDP port number is 0 for the local endpoint of a CEM connection.

Command Modes

CEM xconnect configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

This command does not have a **no** form. To remove a local UPD port number, either configure a new UPD port number or enter the **noxconnect** command to disable the connection and all its parameters.

Examples

The following example demonstrates how to configure the UDP port of the local endpoint of the CEM over IP (CEoIP) connection.

```
Router(config-cem-xconnect)# local udp port 2141
```

Related Commands

Command	Description
remote udp port	Defines the UDP port of the remote endpoint of a CEM connection.
show cem	Displays CEM channel statistics.
xconnect (CEM)	Builds one end of a CEM connection and enters CEM xconnect configuration mode.

local-lnm

To enable Lanoptics Hub Networking Management of a PCbus Token Ring interface, use the **local-lnm** command in interface configuration mode. To disable Lanoptics Hub Networking Management, use the **no** form of this command.

local-lnm commandlocal-lnm
no local-lnm

Syntax Description

This command has no arguments or keywords.

Command Default

Management is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The Token Ring interface on the AccessPro PC card can be managed by a remote LAN manager over the PCbus interface. At present, the Lanoptics Hub Networking Management software running on an IBM compatible PC is supported.

Examples

The following example enables Lanoptics Hub Networking Management:

```
Router(config-if)# local-lnm
```

logging event

To enable notification of interface, subinterface, and Frame Relay data link connection identifier (DLCI) data link status changes, use the **loggingevent** command in interface configuration mode. To disable notification, use the **no** form of this command.

logging event {**dlci-status-change** | **link-status** | **subif-link-status** [**ignore-bulk**]}
no logging event {**dlci-status-change** | **link-status** | **subif-link-status** [**ignore-bulk**]}

Syntax Description

dlci-status-change	Enables notification of Frame Relay DLCI status changes. **Note** This option is supported only when the encapsulation on the interface is Frame Relay.
link-status	Enables notification of interface data link status changes.
subif-link-status	Enables notification of subinterface data link status changes.
ignore-bulk	Suppresses link status messages for subinterfaces when they are caused by a state change of the main interface.

Command Default

For system images, notification of interface, subinterface, and Frame Relay DLCI data link status changes is enabled by default.

For boot images, notification of Frame Relay subinterface and DLCI data link status changes is disabled by default. Notification of interface data link status changes is enabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.0	This command was introduced.
12.2(32)S	The **ignore-bulk** keyword was integrated into the Cisco IOS Release 12.2(32)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.3(7)T	The **ignore-bulk** keyword was integrated into Cisco IOS Release 12.3(7)T.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to enable notification of subinterface link status changes:

```
Router(config-if)# logging event subif-link-status
```

The following are examples of Frame Relay DLCI and subinterface status change notification messages filtered by the **loggingevent** command:

```
00:16:22: %FR-5-DLCICHANGE: Inteface Serial3/0/0:1 - DLCI 105 state changed to INACTIVE
```

```
00:16:22: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/0/0:1.5, changed state
to down
```

logging source-interface

To specify the source IPv4 or IPv6 address of system logging packets, use the **loggingsource-interface** command in global configuration mode . To remove the source designation, use the **no** form of this command.

logging source-interface *type number*
no logging source-interface

Syntax Description

type number	Interface type and number.

Command Default

The wildcard interface address is used.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2	This command was introduced.
12.4(4)T	This command was modified. IPv6 support was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command can be configured on the Virtual Routing and Forwarding (VRF) and non-VRF interfaces. Normally, a syslog message contains the IPv4 or IPv6 address of the interface used to leave the router. The **loggingsource-interface** command configures the syslog packets contain the IP or IPv6 address of a particular interface, regardless of which interface the packet uses to exit the router.

When no specific interface is configured, a wildcard interface address of 0.0.0.0 (for IPv4) or :: (for IPv6) is used, and the IP socket selects the best outbound interface.

Examples

In the following example, the user specifies that the IP address of Ethernet interface 0 is the source IP address for all syslog messages:

```
Router(config)# logging source-interface ethernet 0
```

The following example specifies that the IP address for Ethernet interface 2/1 is the source IP address for all syslog messages:

```
Router(config)# logging source-interface ethernet 2/1
```

The following sample output displays that the **loggingsource-interface** command is configured on a VRF source interface:

```
Router# show running interface loopback49
             Building configuration...
             Current configuration : 84 bytes
```

```
             !
             interface Loopback49
              ip vrf forwarding black
              ip address 49.0.0.1 255.0.0.0
             end
Router# show running | includes logging
      logging source-interface Loopback49 vrf black
      logging host 130.0.0.1 vrf black
```

Related Commands

Command	Description
logging	Logs messages to a syslog server host.

logging event link-status (global configuration)

To change the default or set the link-status event messaging during system initialization, use the **logging event link-status** command in global configuration mode. To disable the link-status event messaging, use the **no** form of this command.

logging event link-status {**default** | **boot**}
no logging event link-status {**default** | **boot**}

Syntax Description

default	Enables system logging of interface state-change events on all interfaces in the system.
boot	Enables system logging of interface state-change events on all interfaces in the system during system initialization.

Command Default

Interface state-change messages are not sent.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You do not have to enter the **logging event link-status boot** command to enable link-status messaging during system initialization. The **logging event link-status default** command logs system messages even during system initialization.

If you enter both the **logging event link-status default** and the **no logging event link-status boot**commands, the interface state-change events are logged after all modules in the Cisco 7600 series router come online after system initialization. The **logging event link-status default** and the **no logging event link-status boot** commands are saved and retained in the running configuration of the system.

When both the **logging event link-status default** and the **no logging event link-status boot**commands are present in the running configuration and you want to display the interface state-change messages during system initialization, enter the **logging event link-status boot** command.

Examples

This example shows how to enable the system logging of the interface state-change events on all interfaces in the system:

```
Router(config)# logging event link-status default
Router(config)#
```

This example shows how to enable the system logging of interface state-change events on all interfaces during system initialization:

```
Router(config)# logging event link-status boot
Router(config)#
```

This example shows how to disable the system logging of interface state-change events on all interfaces:

```
Router(config)# no logging event link-status default
Router(config)#
```

This example shows how to disable the system logging of interface state-change events during system initialization:

```
Router(config)# no logging event link-status boot
Router(config)#
```

Related Commands

Command	Description
show running-config	Displays the status and configuration of the module or Layer 2 VLAN.

logging event link-status (interface configuration)

To enable link-status event messaging on an interface, use the **logging event link-status** command in interface configuration mode. To disable link-status event messaging, use the **no** form of this command.

logging event link-status [{**bchan** | **dchan** | **nfas**}]
no logging event link-status [{**bchan** | **dchan** | **nfas**}]

Syntax Description

bchan	(Optional) Logs B-channel status messages. This keyword is available only for integrated services digital network (ISDN) serial interfaces.
dchan	(Optional) Logs D-channel status messages. This keyword is available only for ISDN serial interfaces.
nfas	(Optional) Logs non-facility associated signaling (NFAS) D-channel status messages. This keyword is available only for ISDN serial interfaces.

Command Default

Interface state-change messages are not sent.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	This command was modified to support the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

To enable system logging of interface state-change events on a specific interface, enter the **logging event link-status** command.

Examples

The following example shows how to enable link-status event messaging on an interface:

```
Router(config-if)# logging event link-status
```

This example shows how to disable link-status event messaging on an interface:

```
Router(config-if)# no logging event link-status
```

logging event subif-link-status

To enable the link-status event messaging on a subinterface, use the **logging event subif-link-status** command in interface configuration mode. To disable the link-status event messaging on a subinterface, use the **no** form of this command.

logging event subif-link-status
no logging event subif-link-status

Syntax Description

This command has no arguments or keywords.

Command Default

Subinterface state-change messages are not sent.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720.

To enable system logging of interface state-change events on a specific subinterface, enter the **logging event subif-link-status** command.

To enable system logging of interface state-change events on a specific interface, enter the **logging event link-status** command.

To enable system logging of interface state-change events on all interfaces in the system, enter the **logging event link-status** command.

Examples

This example shows how to enable the system logging of the interface state-change events on a subinterface:

```
Router(config-if)# logging event subif-link-status
Router(config-if)#
```

This example shows how to disable the system logging of the interface state-change events on a subinterface:

```
Router(config-if)# no logging event subif-link-status
Router(config-if)#
```

Related Commands

Command	Description
show running-config	Displays the status and configuration of the module or Layer 2 VLAN.

logging-events

to print typical T3 controller Up and Down messages on a Channelized T3 Port Adapter**,**use the **logging-eventscommand**in T3 controller configuration mode**.Usethenoformofthiscommandtodisableprintingof theT3controllerUpandDownmessages.**

logging-events [**detail**]
[**no**] **logging-events**

Syntax Description

detail	(Optional) Enables printing the reason code when a T3 controller changes from the Up to Down state.

Command Default

The **logging-eventscommandisthedefault.**

Command Modes

T3 controller configuration

Command History

Release	Modification
12.2(19c)	This command was introduced.

Usage Guidelines

When the no logging-events command disables printing of the T3 controller Up and Down messages, these messages will neither appear on the console nor in the logs.

Examples

The following example uses the **logging-events** [**detail**] command to show the Out-of-Frame (OOF) reason code when the T3 controller changes from an Up state to a Down state:

```
Router(config-controller)# logging-events detail
*Jun 19 17:47:50: %CONTROLLER-5-DOWNDETAIL: Controller T3 4/1, changed state to down due
to OOF
```

Related Commands

Command	Description
t1 logging-events	**Prints the typical T1 controller Up and Down messages** on a channelized T3 port adapter**.**

logging-events (T1-E1 controller)

To show the controller state change and alarms on a controller, use the **logging-events**command in controller configuration mode. To turn off controller state change reporting, use the **no** form of the command.

logging-events *detail*
no logging-events

Syntax Description

detail	Alarm along with the controller state change.

Command Default

Logging-events is the default.

Command Modes

Controller configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced to support SPAs on the Cisco 7600 series router and Catalyst 6500 series switch.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **logging-events**command to show the state change and alarms on a controller on an 8-Port Channelized T1/E1 Serial SPA.

Examples

The following shows enabling the logging-events command.

```
Router(config)#contr e1 2/1/0
Router(config-controller)# logging-events
```

Related Commands

Command	Description
controller	Configures a T1, E1, or T3 controller and enters controller configuration mode.
show controller	Displays controller configuration.

loopback (CEM)

To set the loopback method for testing a T1, E1, serial CEM interface, and VCoP Smart SFP, use the **loopback** command in controller configuration or CEM configuration mode. To remove any existing loopback, use the **no** form of this command.

Cisco NM-CEM-4SER
loopback {**local** | **network**}
no loopback

Cisco NM-CEM-4TE1
loopback {**local** {**payload** | **line**} | **network**}
no loopback

Cisco IOS XE Release 3.18SP
loopback {**diag** | **local** | {**payload** | **line**}}
no loopback

Cisco IOS XE Release 3.18.1SP
loopback {**local** | **network** {**payload** | **line**}}
no loopback

Syntax Description

diag	Loops the outgoing transmit signal back to the receive signal. This is done using the diagnostic loopback feature in the interface module's framer.
local	Places the interface into local loopback mode and creates a loopback wherein information received from the locally-attached customer premises equipment (CPE) is transmitted back to the locally-attached CPE. • **payload** --(Used only if a local loopback is specified for a T1/E1 channel) Creates a loopback of only the data in individual time slots. In this mode, framing bits are terminated and then regenerated instead of being looped back. This mode is not available if the port is configured for **framingunframed**. • **line** --(Used only if a local loopback is specified for a T1/E1 channel) Creates a full physical layer loopback of all bits, including data and framing bits.
network	Creates a loopback wherein data received over the network from the remote CPE is transmitted back to the remote CPE.

Command Default

No loopback is configured for a CEM interface.

Command Modes

CEM configuration

Controller configuration

Controller configuration

Controller configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
XE 3.18SP	This command was integrated in Cisco NCS 4200 Series.
XE 3.18.1SP	This command was integrated in Cisco 900 Series Router.
Cisco IOS XE Everest 16.5.1	This command was integrated in Cisco ASR 903 Series Router and Cisco NCS 4200 Series.

Usage Guidelines

Use this command to create a loopback for a CEM interface. You can use a loopback to test for equipment malfunction caused by the interface.

The NM-CEM-4TE1 does not respond to loopback requests initiated by the CPE, locally attached or remote, using the extended super frame (ESF) Facility Data Link (FDL) mechanism or by any other mechanism.

The NM-CEM-4SER does not respond to any form of loopback request initiated by the locally attached or remote CPE on the Local Loop (LL) or Remote Loop (RL) control leads. Nor does the NM-CEM-4SER respond to any form of loopback request initiated by the locally attached or remote CPE using in-band loopback codes.

Examples

The following example shows how to create a loopback on a CEM T1/E1 interface so that data received from a remote CPE is transmitted back to the remote CPE on the network.

```
Router(config-controller)# loopback network
```

The following example shows how to create a loopback of data in individual time slots on a CEM T1/E1 interface. Data received from a locally attached CPE will be sent back to the locally attached CPE.

```
Router(config-controller)# loopback local payload
```

The following example shows how to create a loopback on a serial CEM channel so that data received from a remote CPE is transmitted back to the remote CPE on the network.

```
Router(config-cem)# loopback network
```

The following example shows how to set a loopback on the T1 interfaces for loopback diag.

```
Router(config-controller)# loopback diag
```

The following example shows how to set a loopback on the C37.94 interface for loopback local.

```
Router(config-controller)# loopback local line
```

Related Commands

Command	Description
cem	Enters circuit emulation configuration mode.
controller	Enters controller configuration mode.

loopback (DSL controller)

To test the controller and configure the core loopback, use the **loopback(DSLController)**command in controller configuration mode. To remove the loopback interface, use the **no** form of this command.

loopback {**analog** | **digital**}
no loopback

Syntax Description

analog	Loops the circuit at the analog hybrid to verify the analog loopback hardware to the analog hybrid.
digital	Loops the circuit at the framer to verify the hardware to the framer.

Command Default

No default behavior or values.

Command Modes

Controller configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced on Cisco 2600 series and Cisco 3700 series routers.
12.3(4)XG	This command was integrated into Cisco IOS Release 12.3(4)XG on the Cisco 1700 series routers.
12.3(7)T	This command was integrated in Cisco IOS Release 12.3(7)T on Cisco 2600 series, Cisco 3631, and Cisco 3700 series routers.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T on Cisco 2800 series and Cisco 3800 series routers.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T on Cisco 1800 series routers.

Usage Guidelines

Analog and digital loopbacks are local loopbacks. Digital loopbacks loop the circuit at the framer to verify the hardware to the framer, and analog loopbacks loop the circuit at the analog hybrid to verify the analog loopback hardware to the analog hybrid. The controller must be shut down before loopback can be configured.

Examples

If the controller is still up, the router will prompt you to turn the controller off as shown in this example:

```
Router(config-controller)# loopback
 analog

 Please shut down the xDSL controller
Router(config-controller)# loopback
 digital

 Please shut down the xDSL controller
```

The following example shows the configuration of a loopback digital interface:

```
Router(config-controller)# loopback digital
 Please shut down the xDSL controller
Router(config-controller)# shutdown
```

```
Router(config-controller)#
00:59:50: %CONTROLLER-5-UPDOWN: Controller DSL 0/0, changed state to
administratively down
Router(config-controller)#
Router(config-controller)# loopback digital
Router(config-controller)# no shutdown
Apr 23 06:59:01.435:  DSL 0/0 controller Link up! line rate: 4608 Kbps
o
00:59:59: %CONTROLLER-5-UPDOWN: Controller DSL 0/0, changed state to up
Router(config-controller)#end
Router# show controllers dsl 0/0
 DSL 0/0 controller UP
 Local Digital loopback is running
 Globespan xDSL controller chipset
 DSL mode: SHDSL Annex B
 Frame mode: Utopia
 Configured Line rate: 4608Kbps
 Line Re-activated 4 times after system bootup
 LOSW Defect alarm: ACTIVE
 CRC per second alarm: ACTIVE
 Line termination: CO
 FPGA Revision: 0xA7
Line 0 statistics
        Current 15 min CRC: 679
        Current 15 min LOSW Defect: 8
        Current 15 min ES: 5
        Current 15 min SES: 5
        Current 15 min UAS: 397
        Previous 15 min CRC: 0
        Previous 15 min LOSW Defect: 0
        Previous 15 min ES: 0
        Previous 15 min SES: 0
        Previous 15 min UAS: 0
Line 1 statistics
        Current 15 min CRC: 577
        Current 15 min LOSW Defect: 8
        Current 15 min ES: 7
        Current 15 min SES: 4
        Current 15 min UAS: 411
        Previous 15 min CRC: 0
        Previous 15 min LOSW Defect: 0
        Previous 15 min ES: 0
        Previous 15 min SES: 0
        Previous 15 min UAS: 0
 Line-0 status
 Chipset Version:  1
 Firmware Version:  A29733
 Modem Status:  un checked mode, Status 83
 Last Fail Mode:  No Failure status:0x0
 Line rate:  2312 Kbps
 Framer Sync Status: In Sync
 Rcv Clock Status: In the Range
 Loop Attenuation:  0.0 dB
 Transmit Power:  13.5 dB
 Receiver Gain:  936.8420 dB
 SNR Sampling:  16.960 dB
 Line-1 status
 Chipset Version:  1
 Firmware Version:  A29733
 Modem Status:  un checked mode, Status 83
 Last Fail Mode:  No Failure status:0x0
 Line rate:  2312 Kbps
 Framer Sync Status: In Sync
 Rcv Clock Status: In the Range
```

```
Loop Attenuation:  0.0 dB
Transmit Power:  13.5 dB
Receiver Gain:  936.8420 dB
SNR Sampling:  16.3590 dB
Dying Gasp: Present
```

Related Commands

Command	Description
show interfaces loopback	Displays information about the loopback interface.

loopback (E3 controller)

To loop an entire E3 line toward the line and back toward the router, use the **loopback**command in controller configuration mode. To remove the loop, use the no form of this command.

loopback {**local** | **network** {**line** | **payload**}}
no loopback

Syntax Description

local	Loops the data back toward the router and sends an AIS signal out toward the network. This is the default.
network line payload	Sets the loopback toward the network either before going through the framer (line) or after going through the framer (payload).

Command Default

local

Command Modes

Controller configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(11)YT	This command was integrated into Cisco IOS Release 12.2(11)YT and implemented on the following platforms for E3: Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3660 series, Cisco 3725, and Cisco 3745 routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines

Use this command for troubleshooting purposes. To verify that a loopback is configured on the interface, use the **showcontrollerse3**EXEC command. Note that line loopback is available only in C-bit parity mode.

Examples

The following example shows how to configure the controller located in slot 1, port 0 for a local loopback:

```
Router(config)# controller e3 1/0
Router(config-controller)# loopback local
```

Related Commands

Command	Description
show controllers e3	Displays information about the E3 controllers.

loopback (interface)

To diagnose equipment malfunctions between the interface and device, use the **loopback**command in interface configuration mode. To disable the test, use the **no** form of this command.

loopback
no loopback

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Loopback on HSSI Cards

On High-Speed Serial Interface (HSSI) cards, the loopback function configures a two-way internal and external loop on the HSA applique of the specific interface.

Loopback on MCI and SCI Serial Interface Cards

On MCI and SCI serial interface cards, the loopback functions when a CSU/DSU or equivalent device is attached to the router or access server. The**loopback** command loops the packets through the CSU/DSU to configure a CSU loop, when the device supports this feature.

Loopback on MCI and MEC Ethernet Cards

On the MCI and MEC Ethernet cards, the interface receives back every packet it sends when the **loopback** command is enabled. Loopback operation has the additional effect of disconnecting network server functionality from the network.

Loopback on CSC-FCI FDDI Cards

On the CSC-FCI FDDI card, the interface receives back every packet it sends when the **loopback** command is enabled. Loopback operation has the additional effect of disconnecting network server functionality from the network.

Loopback on Token Ring Interface Cards

On all Token Ring interface cards (except the 4-megabit CSC-R card), the interface receives back every packet it sends when the **loopback** command is enabled. Loopback operation has the additional effect of disconnecting network server functionality from the network.

Active Loopback Interfaces

To show interfaces currently in loopback operation, use the **showinterfacesloopback** EXEC command.

Note Loopback does not work on an X.21 DTE because the X.21 interface definition does not include a loopback definition.

Examples

The following example configures the loopback test on Ethernet interface 4:

```
Router(config)# interface ethernet 4
Router(config-if)# loopback
```

Related Commands

Command	Description
down-when-looped	Configures an interface to inform the system it is down when loopback is detected.
show interfaces loopback	Displays information about the loopback interface.

loopback (J1 controller)

To set the loopback method for testing the J1 interface, use the **loopback** command in controller configuration mode. To turn off loopback, use the **no** form of this command. This command should be used for testing purposes only.

loopback {**local** | **line** | **isolation**}
no loopback {**local** | **line** | **isolation**}

Syntax Description

local	Places the interface into local loopback mode.
line	Places the interface into external loopback mode at the line level.
isolation	Places the interface into both local and line loopback mode.

Command Default

No loopback is configured.

Command Modes

Controller configuration

Command History

Release	Modification
11.3 MA	This command was implemented on the Cisco MC3810.
12.0(5)T and 12.0(7)XR	The command was implemented on the Cisco 2600 and Cisco 3600 series.
12.0(5)XE	The command was implemented on the Cisco 7200 and Cisco 7500 series.
12.1(1)T	The command was implemented on the Cisco 2600 series.
12.2(8)T	The command was implemented on the Cisco 2600 and Cisco 3600 series.

Examples

The following example establishes a loopback of the incoming J1 signal on controller J1 3/0:

```
Router(config)# controller j1 3/0
Router(config-controller)# loopback line
```

loopback (PA-MC-8TE1+ port adapter)

To enable loopback testing of data for the PA-MC-8TE1+ port adapter, use the **loopback** command in interface configuration mode. To disable loopback testing, use the **no** form of this command.

loopback [{**internal** | **line**}]
no loopback [{**internal** | **line**}]

Syntax Description

internal	(Optional) Loops any data received at the PA-MC-8TE1+ port adapter's network interface back into the PA-MC-8TE1+ port adapter.
line	(Optional) Loops any data received at the PA-MC-8TE1+ port adapter's network interface back into the network.

Command Default

Loopback mode is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Examples

In the following example, a loopback is set for the PA-MC-8TE1+ port adapter in slot 2:

```
Router(config)# interface 2/0
Router(config-if)# loopback line
```

loopback T1 interface through nrzi-encoding

loopback (T1 interface)

To loop individual T1 channels on the CT3IP in Cisco 7000 series routers that have the RSP7000 and RSP7000CI and in Cisco 7500 series routers, use the **loopback**command in interface configuration mode. To remove the loopback, use the **no** form of this command.

loopback [{**local** | **network** {**line** | **payload**} | **remote** {**line** {**fdl** {**ansi** | **bellcore**} | **inband**} | **payload** [**fdl**] [**ansi**]}}]
no loopback

Syntax Description

local	(Optional) Loops the router output data back toward the router at the T1 framer and sends an alarm indication signal (AIS) signal out toward the network.
network line | **payload**	(Optional) Loops the data back toward the network before the T1 framer and automatically sets a local loopback at the High-Level Data Link Control (HDLC) controllers (line), or loops the payload data back toward the network at the T1 framer and automatically sets a local loopback at the HDLC controllers (payload).
remote l**inefdl** {**ansi**|**bellcore**	(Optional) Sends a repeating, 16-bit Extended Superframe (ESF) data link code word (00001110 11111111 for FDL ANSI and 00010010 11111111 for FDL Bellcore) to the remote end requesting that it enter into a network line loopback. Specify the **ansi** keyword to enable the remote line Facility Data Link (FDL) ANSI bit loopback on the T1 channel, per the ANSI T1.403 specification. Specify the **bellcore** keyword to enable the remote SmartJack loopback on the T1 channel, per the TR-TSY-000312 specification.
remote line inband	(Optional) Sends a repeating, 5-bit inband pattern (00001) to the remote end requesting that it enter into a network line loopback.
remote payload [**fdl**] [**ansi**]	(Optional) Sends a repeating, 16-bit ESF data link code word (00010100 11111111) to the remote end requesting that it enter into a network payload loopback. Enables the remote payload FDL ANSI bit loopback on the T1 channel. You can optionally specify **fdl** and **ansi**, but it is not necessary.

Command Default

No loopback is configured.

Command Modes

Interface configuration

Command History

Release	Modification
11.1 CA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command for troubleshooting purposes.

To better diagnose T1 provisioning problems, you can place the remote CSU or remote SmartJack into loopback. The **loopbackremotelinefdl** interface configuration command allows you to place either the CSU or the SmartJack into loopback:

- **ansi** --Places the CSU into loopback, per the ANSI T1.403 Specification.
- **bellcore** --Places the SmartJack into loopback, per the TR-TSY-000312 Specification.

When both are configured, transmission of loss of frame (LOF) indication (yellow alarm) takes priority over transmission of some facilities data link (FDL) messages.

If the remote loopback appears not to be working, use the show controllers t3 command to determine if the given T1 is currently attempting to transmit a LOF indication (yellow alarm):

```
Router#
show controllers t3 0/0/0:2
T3 0/0/0 is up.
   CT3 H/W Version: 5, CT3 ROM Version: 1.2, CT3 F/W Version: 2.5.9
   Mx H/W version: 2, Mx ucode ver: 1.34

   T1 2 is down, speed: 1536 kbs, non-inverted data
   timeslots: 1-24
   FDL per AT&T 54016 spec.
   Transmitter is sending LOF Indication.
   Receiver is getting AIS.
```

If the transmitter is sending a LOF indication, as in the previous example, stop the transmission of the LOF indication (yellow alarm) with the no t1 yellow generation configuration command as shown in the following example:

```
Router(config)# controllers t3 0/0/0
Router(config-controller)# no t1 2 yellow generation
Router(config-controller)# Ctrl-D
```

To verify that the transmission of the LOF indication (yellow alarm) has stopped, use the show controllers t3 command:

```
Router# show controllers t3 0/0/0:2
T3 0/0/0 is up.
   CT3 H/W Version: 5, CT3 ROM Version: 1.2, CT3 F/W Version: 2.5.9
   Mx H/W version: 2, Mx ucode ver: 1.34
   T1 2 is down, speed: 1536 kbs, non-inverted data
   timeslots: 1-24
   FDL per AT&T 54016 spec.
   Receiver is getting AIS.
   Framing is ESF, Line Code is B8ZS, Clock Source is Internal.
   Yellow Alarm Generation is disabled
```

Then retry the remote loopback command. When diagnosis is complete, remember to reenable the LOF indication (yellow alarm).

You can also loopback all the T1 channels by using the**loopback**(CT3IP) interface configuration command.

Examples

The following example configures T1 channel 5 for a local loopback:

```
Router(config)# interface serial 3/0/0:5
Router(config-if)# loopback local
```

Related Commands

Command	Description
loopback (T3 controller)	Loops the entire T3 (all 28 T1 channels) on the CT3IP in Cisco 7500 series routers.
t1 yellow generation	Enables detection and generation of yellow alarms for a T1 channel on the CT3IP in Cisco 7500 series routers.

loopback (T3/E3 controller)

To loop the entire T3 (all 28 T1 channels) line on the T3 controller or E3 (all 16 E1 channels) in Cisco NCS 4200 Series or on the CT3IP in Cisco 7500 series routers, use the **loopback** command in controller configuration mode. To remove the loop, use the **no** form of this command.

loopback {**local** | **network** {**line** | **payload**} | **remote**}
no loopback

Syntax Description

local	Loops the data back toward the router and sends an alarm indication signal (AIS) out toward the network.
network line payload	Sets the loopback toward the network either before going through the framer (line) or after going through the framer (payload).
remote	Sends a far-end alarm control (FEAC) request to the remote end requesting that it enter into a network line loopback. FEAC requests (and therefore remote loopbacks) are possible only when the T3 is configured for C-bit framing. The M23 format does not support remote loopbacks.

Command Default

No loops are configured on the T3/E3 line.

Command Modes

Controller configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(11)YT	This command was integrated into Cisco IOS Release 12.2(11)YT and implemented on the following platforms for T3: Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3660 series, Cisco 3725, and Cisco 3745 routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
XE 3.18SP	This command was integrated into Cisco NCS 4200 Series.
XE Everest 16.5.1	This command was integrated into Cisco NCS 4200 Series and Cisco ASR 900 Series Routers.

Usage Guidelines

Use this command for troubleshooting purposes. To verify that a loopback is configured on the interface, use the **showcontrollersT3/E3**EXEC command. Note that remote loopback is available only in C-bit parity mode.

You can also loopback each T1/E1 channel by using the**loopback** interface configuration command for T1/E1.

For more information, refer to the "Troubleshooting the T3 and T1 Channels" section in the "Configuring Serial Interfaces" chapter of the *CiscoIOSInterfaceandHardwareComponentConfigurationGuide*.

Examples

The following example configures the T3/E3 or CT3IP for a local loopback:

```
Router(config)# controller t3/e3 3/0/0
Router(config-controller)# loopback local
```

Related Commands

Command	Description
framing	Selects the frame type for the T1 or E1 data line.
loopback (interface)	Places the specified module in loopback mode.
loopback remote (interface)	Loops packets through a CSU/DSU, over a DS3 link or a channelized T1 link, to the remote CSU/DSU and back.
show controllers t3/e3	Displays information about the T3/E3 controllers.

loopback (T3-E3 interface)

To loopback at various points in the transmit and receive path, use the **loopback**command in interface configuration mode. To stop the loopback, use the no form of this command.

PA-T3 Port Adapter
loopback {**dte** | **local** | **network** {**line** | **payload**} | **remote**}
no loopback

PA-E3 Port Adapter
loopback {**dte** | **local** | **network** {**line** | **payload**}}
no loopback

T3/E3 Shared Port Adapters
loopback {**dte** | **local** | **dual** | **network** {**line** | **payload**} | **remote**}
no loopback {**dte** | **local** | **dual** | **network** {**line** | **payload**} | **remote**}

Syntax Description

dte	Loopback after the line interface unit (LIU) towards the terminal.
local	Loopback after going through the framer toward the terminal.
dual	Sets both local loopback and network line loopback. The dual keyword is not supported on Cisco 7304 routers with the 2-Port and 4-Port Channelized T3 SPA.
network line | **payload**	Sets the loopback toward the network before going through the framer (**line**) or after going through the framer (**payload**).
remote	Sends FEAC to set remote in loopback.

Command Default

No loopback by default.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
11.3	This command was introduced.
12.2(11)YT	This command was integrated into Cisco IOS Release 12.2(11)YT and implemented on the following platforms for E3: Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3660 series, Cisco 3725, and Cisco 3745 routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2S	This command was integrated into Cisco IOS Release 12.2S.
12.2(25)S3	This command was integrated into Cisco IOS Release 12.2(25)S3 to support SPAs on the Cisco 7304 routers.

Release	Modification
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE to support SPAs on the Cisco 7600 series routers and Catalyst 6500 series switches. The **dual** keyword was added.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S to support SPAs on Cisco 12000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the loopback command to diagnose problems on the local port, between the framer and the line interface unit (LIU) level.

To verify that a loopback is configured on the interface, use the **showinterfacesserial** or **showinterfacesloopback** command.

The dual keyword is not supported on Cisco 7304 routers with the 2-Port and 4-Port Channelized T3 SPA.

Examples

The following example configures the serial interface located in slot 3/0/0 for a local loopback:

```
Router(config)# interface serial 3/0/0
Router(config-if)# loopback local
```

The following example creates a loopback on slot 5, bay 0 after the LIU towards the terminal.

```
Router# configure terminal
Router(config)# interface serial 5/0/0
Router(config-if)# loopback dte
```

Related Commands

Command	Description
show controllers serial	Displays information that is specific to the interface hardware.
show interfaces loopback	Displays information about the loopback interface.
show interfaces serial	Displays information about a serial interface.

loopback applique

To configure an internal loop on the High-Speed Serial Interface (HSSI) applique, use the **loopbackapplique** command in interface configuration mode. To remove the loop, use the **no** form of this command.

loopback applique commandloopback applique
no loopback applique

Syntax Description

This command has no arguments or keywords.

Command Default

No loops are configured on the HSSI applique.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command loops the packets within the applique to provide a way to test communication within the router or access server. It is useful for sending pings to yourself to check functionality of the applique.

To show a specific interface that is currently in loopback operation, use the **showinterfacesloopback** EXEC command.

Examples

The following example configures the loopback test on the HSSI applique:

```
Router(config)# interface serial 1
Router(config-if)# loopback applique
```

Related Commands

Command	Description
show interfaces loopback	Displays information about the loopback interface.

loopback dte

To loop packets back to the DTE from the CSU/DSU, when the device supports this function, use the **loopbackdte**command in interface configuration mode. To remove the loop, use the **no** form of this command.

loopback dte commandloopback dte
no loopback dte

Syntax Description

This command has no arguments or keywords.

Command Default

No loops are configured.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is useful for testing the DTE-to-DCE cable.

This command is used to test the performance of the integrated CSU/DSU. Packets are looped from within the CSU/DSU back to the serial interface of the router. Send a test ping to see if the packets successfully looped back. To cancel the loopback test, use the **noloopbackdte** command.

When using the 4-wire 56/64-kbps CSU/DSU module, an out-of-service signal is transmitted to the remote CSU/DSU.

To show a specific interface that is currently in loopback operation, use the**showinterfacesloopback** EXEC command.

Examples

The following example configures the loopback test on the DTE interface:

```
Router(config)# interface serial 0
Router(config-if)# loopback dte
```

Related Commands

Command	Description
show interfaces loopback	Displays information about the loopback interface.

loopback line

To loop packets completely through the CSU/DSU to configure the CSU loop, use the **loopbackline** command in interface configuration mode. To remove the loop, use the **no** form of this command.

loopback line [**payload**]
no loopback line [**payload**]

Syntax Description

payload	(Optional) Configures a loopback point at the DSU and loops data back to the network on an integrated CSU/DSU.

Command Default

No loops are configured.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is useful for testing the DCE device (CSU/DSU) itself. When the **loopbackline** command is configured on the 2-wire 56-kbps CSU/DSU module or the 4-wire 56/64-kbps CSU/DSU modules, the network data loops back at the CSU and the router data loops back at the DSU. If the CSU/DSU is configured for switched mode, you must have an established connection to perform a payload-line loopback. To loop the received data through the minimum amount of CSU/DSU circuitry, issue the **loopbackline** command.

When you issue the **loopbacklinepayload** command on an integrated CSU/DSU module, the router cannot transmit data through the serial interface for the duration of the loopback. Choosing the DSU as a loopback point loops the received-network data through the maximum amount of CSU/DSU circuitry. Data is not looped back to the serial interface. An active connection is required when operating in switched mode for payload loopbacks.

If you enable the **loopbackline** command on the fractional T1/T1 module, the CSU/DSU performs a full-bandwidth loopback through the CSU portion of the module and data transmission through the serial interface is interrupted for the duration of the loopback. No reframing or corrections of bipolar violation errors or cyclic redundancy check (CRC) errors are performed. When you configure the **loopbacklinepayload**command on the FT1/T1 module, the CSU/DSU performs a loopback through the DSU portion of the module. The **loopbacklinepayload**command reframes the data link, regenerates the signal, and corrects bipolar violations and Extended Super Frame CRC errors.

When performing a T1-line loopback with Extended Super Frame, communication over the facilities data link is interrupted, but performance statistics are still updated. To show interfaces currently in loopback operation, use the **showservice-module**EXEC command.

To show interfaces that are currently in loopback operation on other routers, use the **showinterfacesloopback** EXEC command.

Examples

The following example configures the loopback test on the DCE device:

```
Router(config)# interface serial 1
Router(config-if)# loopback line
```

The following example shows how to configure a payload loopback on a Cisco 2524 or Cisco 2525 router:

```
Router1(config-if)# loopback line payload
Loopback in progress
Router1(config-if)# no loopback line
```

The following example shows the output on a Cisco 2524 or Cisco 2525 router when you loop a packet in switched mode without an active connection:

```
Router1(config-if)# service-module 56k network-type switched
Router1(config-if)# loopback line payload
Need active connection for this type of loopback
% Service module configuration command failed: WRONG FORMAT.
```

Related Commands

Command	Description
show interfaces loopback	Displays information about the loopback interface.
show service-module	Displays the performance report for an integrated CSU/DSU.

loopback remote (interface)

To loop packets through a CSU/DSU, over a DS3 link or a channelized T1 link, to the remote CSU/DSU and back, use the **loopbackremote**command in interface configuration mode. To remove the loopback, use the **no** form of this command.

FT1/T1 CSU/DSU Modules

loopback remote {**full** | **payload** | **smart-jack**} [{**0in1** | **1in1** | **1in2** | **1in5** | **1in8** | **3in24** | **qrw** | **user-pattern** *24-bit-binary-value*}]

no loopback remote {**full** | **payload** | **smart-jack**}

2- and 4-Wire, 56/64-kbps CSU/DSU Modules

loopback remote [{**2047** | **511** | **stress-pattern** *pattern-number*}]

no loopback remote

Syntax Description

full	Transmits a full-bandwidth line loopback request to a remote device, which is used for testing.
payload	Transmits a payload line loopback request to a remote device, which is used for testing the line and remote DSU.
smart-jack	Transmits a loopback request to the remote smart jack, which some service providers attach on the line before the customer premises equipment (CPE). You cannot put the local smart jack into loopback.
0in1	(Optional) Transmits an all-zeros test pattern used for verifying B8ZS line encoding. The remote end might report a loss of signal when using alternate mark inversion (AMI) line coding.
1in1	(Optional) Transmits an all-ones test pattern used for signal power measurements.
1in2	(Optional) Transmits an alternating ones-and-zeroes test pattern used for testing bridge taps.
1in5	(Optional) Transmits the industry-standard test-pattern loopback request.
1in8	(Optional) Transmits a test pattern used for stressing timing recovery of repeaters.
3in24	(Optional) Transmits a test pattern used for testing the ones density tolerance on AMI lines.
qrw	(Optional) Transmits a quasi-random word test pattern, which is a random signal that simulates user data.
user-pattern *24-bit-binary-value*	(Optional) Transmits a test pattern that you define. Enter a binary string up to 24 bits long. For the fixed patterns such **0in1** and **1in1**, the T1 framing bits are jammed on top of the test pattern; for the **user-pattern**, the pattern is simply repeated in the time slots.
2047	(Optional) Transmits a pseudorandom test pattern that repeats after 2047 bits.
511	(Optional) Transmits a pseudo random test pattern that repeats after 511 bits.

stress-pattern *pattern-number*	(Optional) Transmits a DDS stress pattern available only on the 4-wire 56/64-kbps CSU/DSU module. You may enter a stress pattern from 1 to 4. A 1 pattern sends 100 bytes of all 1s and then 100 bytes of all 0s to test the stress clocking of the network. A 2 pattern sends 100 bytes of a 0x7e pattern and then 100 bytes of all 0s. A 3 pattern sends continuous bytes of a 0x46 pattern. A 4 pattern sends continuous bytes of a 0x02 pattern.

Command Default

No remote loopback interface is configured.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is used for testing the data communication channels along with or without remote CSU/DSU circuitry. The loopback is usually performed at the line port, rather than the DTE port, of the remote CSU/DSU.

For a multiport interface processor connected to a network via a channelized T1 link, the **loopbackremote** interface configuration command applies if the remote interface is served by a DDS line (56 kbps or 64 kbps) and if the device at the remote end is a CSU/DSU. In addition, the CSU/DSU at the remote end *must* react to latched DDS CSU loopback codes. Destinations that are served by other types of lines or that have CSU/DSUs that do not react to latched DDS CSU codes cannot participate in an interface remote loopback. Latched DDS CSU loopback code requirements are described in AT&T specification TR-TSY-000476, "OTGR Network Maintenance Access and Testing."

For the integrated FT1/T1 CSU/DSU module, the **loopbackremotefull** command sends the loopup code to the remote CSU/DSU. The remote CSU/DSU performs a full-bandwidth loopback through the CSU portion of the module. The**loopbackremotepayload** command sends the loopup code on the configured time slots, while maintaining the D4-extended super frame. The remote CSU/DSU performs the equivalent of a loopback line payload request. The remote CSU/DSU loops back only those time slots that are configured on the remote end. This loopback reframes the data link, regenerates the signal, and corrects bipolar violations and extended super frame CRC errors. The **loopbackremotesmart-jack**command sends a loopup code to the remote smart jack. You cannot put the local smart jack into loopback.

Failure to loopup or initiate a remote loopback request could be caused by enabling the **noservice-modulet1remote-loopback** command or having an alternate remote-loopback code configured on the remote end. When the loopback is terminated, the result of the pattern test is displayed.

For the 2- and 4-wire, 56/64-kbps CSU/DSU module, an active connection is required before a loopup can be initiated while in switched mode. When transmitting V.54 loopbacks, the loopback mode is initiated on the remote device using V.54 messages. Failure to loopup or initiate a remote loopback request could be caused by enabling the **noservice-module56kremote-loopback** command.

To display interfaces that are currently in loopback operation, use the **showinterfacesloopback** EXEC command.

Examples

Example for Remote Loopback Test

The following example configures a remote loopback test:

```
Router(config)# interface serial 0

Router(config-if)# loopback remote
```

Example of Full-Bandwidth Line Loopback

The following example configures the remote device into full-bandwidth line loopback while specifying the **qrw** test pattern over the T1 CSU/DSU module on a Cisco 2524 or Cisco 2525 router:

```
Router(config)# interface serial 0
Router(config-if)# loopback remote full qrw
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state to down
%LINK-3-UPDOWN: Interface Serial0, changed state to down
%SERVICE_MODULE-5-LOOPUPREMOTE: Unit 0 - Remote unit placed in loopback
```

Example of Loopback Stress Pattern

The following example transmits a remote loopback stress pattern over the 4-wire, 56/64-kbps CSU/DSU module, which tests the stress clocking of the network:

```
Router(config-if)# loopback remote stress-pattern 1
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1, changed state to down
%LINK-3-UPDOWN: Interface Serial1, changed state to down
%SERVICE_MODULE-5-LOOPUPREMOTE: Unit 1 - Remote unit placed in loopback
```

Related Commands

Command	Description
clear service-module serial	Resets an integrated CSU/DSU.
loopback dte	Loops packets back to the DTE device from the CSU/DSU.
loopback line	Loops packets completely through the CSU/DSU to configure the CSU loop.
service-module 56k remote-loopback	Enables the acceptance of a remote loopback request on a serial interface on a 2- or 4-wire, 56/64-kbps CSU/DSU module.
service-module t1 remote-loopback	Specifies whether the fractional T1/T1 CSU/DSU module enters loopback mode when it receives a loopback code on the line.
show interfaces loopback	Displays information about the loopback interface.
show service-module serial	Displays the performance report for an integrated CSU/DSU.

loopback remote (T1/T3/SDH/SONET Controller)

To put the far-end T1 or T3 interfaces into a loopback use the **loopback remote** command in the global configuration mode.The remote loopback setting loops back the far-end at line or payload, using inband bit-orientated CDE (IBOC) or the extended super frame (ESF) loopback codes to communicate the request to the far-end.

T1 Controller
loopback remote {esf | {line {csu} | payload} iboc {fac1 | fac2 | csu}}

T3 Controller
loopback remote {line | payload}

Syntax Description

esf line csu	Remote line CSU loopback through FDL. This is the default option.
esf payload	Remote payload loopback through FDL.
iboc fac1	Remote inband line facility1 loopback.
iboc fac2	Remote inband line facility2 loopback.
iboc csu	Remote inband line CSU loopback.

Command Default

Loopback remote is disabled.

Command Modes

Global configuration mode

Command History

Release	Modification
IOS XE Fuji Release 16.8.1	This command was introduced.

Usage Guidelines

Loopback testing is one of the troubleshooting methods which is an effective way to isolate the failing links. When the loopback is configured, all the data sent is received back. If the same data is not received then it is declared as link failure. In the similar way, remote loopback is configured to troubleshoot the link failure between two nodes.

Examples

The following example shows how to set T1 loopback remote iboc fac1 for DS1:

```
Router(config)# controller t1 0/0/1
Router(config-controller)#loopback remote iboc fac1
exit
```

The following example shows how to set T3 loopback remote line for DS3:

```
Router(config)# controller t3 0/0/1
Router(config-controller)#loopback remote line
exit
```

The following example shows how to set T3 loopback remote payload for OCX in sonet:

```
Router(config)# controller sonet 0/0/1
Router(config-controller)#sts 1
Router(config-ctrlr-sts1)#mode t3
Router(config-ctrlr-sts1)#t3 loopback remote payload
```

The following example shows how to set T1 loopback remote esf line csu for OCX in SDH:

```
Router(config)#controller sdh 0/4/7
Router(config-controller)#au-4 1
Router(config-ctrlr-tug3)#tug-3 3
Router(config-ctrlr-tug3)#mode vc1x
Router(config-ctrlr-tug3)#tug-2 1 payload vc11
Router(config-ctrlr-tug2-vcx)#t1 1 loopback remote esf line csu
```

Related Commands

Commands	URL
card type	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-c1.html#wp2336574570
cem-group	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-c1.html#wp2440628600
payload-size dejitter-buffer	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-o1.html#wp3946673156
class cem	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-c1.html#wp2169323859
controller t1/e1	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-c2.html#wp1472647421
xconnect	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-t2.html#wp8578094790
linecode	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-l1.html#wp2312535965
framing	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-f1.html#wp2853515177
clock source	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-c2.html#wp6081785140

Commands	URL
cable length	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-c1.html#wp2492964151
bert pattern	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-a1.html#wp3620978929
channelized	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-c1.html#wp7026926390
loopback	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-l1.html#wp1033903426
show controller t1	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-s3.html#wp2149471094
show controller e1	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-s2.html#wp1632676058

loopback (SONET)

To set the loopback method for testing an interface, use the **loopback** command in the controller configuration mode. To reset to the default, use the **no** form of this command.

loopback [*local* | *network* {*line* | *payload*}]

Syntax Description

local	The name of a CEM interface parameters class.
network {*line* | *payload*	Sets the loopback toward the network before going through the framer (*line*) or after going through the framer (*payload*).

Command Default

No loopback is configured.

Command Modes

Controller configuration

Command History

Release	Modification
3.18 SP	Support for this command was introduced on NCS 4200 Series.

Usage Guidelines

You can use a loopback test on lines to detect and distinguish equipment malfunctions caused by the line. If correct data transmission is not possible when an interface is in loopback mode, the interface is the source of the problem.

Examples

The following example shows the configuration of VT 1.5-T1 loopback :

```
enable
configure terminal
controller MediaType 0/5/0
mode sonet
controller sonet 0/5/0
loopback local
sts-1 1
mode ct3
vtg 1 t1 1 loopback line
end
```

Related Commands

Command	Description
controller sonet	Configures the SONET mode.
show controller sonet	Displays SONET controller configuration.

mac-address-table learning

To enable MAC-address learning, use the **mac-address-tablelearning**command in global configuration mode. To disable learning, use the **no** form of this command.

`mac-address-table learning`{`vlan`*vlan-id* | `interface`*interface slot/port*} {`module`[*module num*]}

`no mac-address-table learning`{`vlan`*vlan-id* | `interface`*interface slot/port*} {`module`[*module num*]}

Syntax Description

default	(Optional) Returns to the default settings.
vlan *vlan-id*	Specifies the VLAN to apply the per-VLAN learning of all MAC addresses; valid values are from 1 to 4094.
interface	Specifies per-interface based learning of all MAC addresses.
interface slot / port	Interface type, the slot number, and the port number.
module *num*	(Optional) Specifies the module number.

Command Default

If you configure a VLAN on a port in a module, all the supervisor engines and Distributed Forwarding Cards (DFCs) in the Cisco 7600 series router are enabled to learn all the MAC addresses on the specified VLAN.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You can use the **module***num* keyword and argument to specify supervisor engines or DFCs only.

You can use the **vlan***vlan-id* keyword and argument on switch-port VLANs only. You cannot use the **vlan***vlan-id* keyword and argument to configure learning on routed interfaces.

You can use the **interface***interfaceslot/port* keyword and arguments on routed interfaces, supervisor engines, and DFCs only. You cannot use the **interface***interfaceslot/port* keyword and arguments to configure learning on switch-port interfaces or non-DFC modules.

Examples

This example shows how to enable MAC-address learning on a switch-port interface on all modules:

```
Router(config)# mac-address-table learning vlan 100
Router(config)#
```

This example shows how to enable MAC-address learning on a switch-port interface on a specified module:

```
Router(config)# mac-address-table learning vlan 100 module 4
Router(config)#
```

This example shows how to disable MAC-address learning on a specified switch-port interface for all modules:

```
Router(config)# no mac-address-table learning vlan 100
Router(config)#
```

This example shows how to enable MAC-address learning on a routed interface on all modules:

```
Router(config)# mac-address-table learning vlan 100
Router(config)#
```

This example shows how to enable MAC-address learning on a routed interface for a specific module:

```
Router(config)# mac-address-table learning interface FastEthernet 3/48 module 4
Router(config)#
```

This example shows how to disable MAC-address learning for all modules on a specific routed interface:

```
Router(config)# no mac-address-table learning interface FastEthernet 3/48
Router(config)#
```

Related Commands

Command	Description
show mac-address-table learning	Displays the MAC-address learning state.

mac-address (virtual switch)

To specify a Media Access Control (MAC) address to use as the common router MAC address for interfaces on the active and standby chassis, use the **mac-address** virtual switch configuration submode command. To return to the default setting, use the **no** form of this command.

mac-address {*mac-address* | **use-virtual**}

Syntax Description

mac-address	MAC address in hexadecimal format.
use-virtual	Specifies the MAC address range reserved for the virtual switch system (VSS).

Command Default

The router MAC address is derived from the backplane of the active chassis.

Command Modes

Virtual switch configuration submode (config-vs-domain)

Command History

Release	Modification
12.2(33)SXH2	Support for this command was introduced.

Usage Guidelines

When a virtual switch comes up, the router MAC address is derived from the backplane of the active chassis and is used as the common router MAC address for interfaces on both the active and the standby chassis. Between switchovers, this MAC address is maintained on the new active switch. You can enter the **mac-address***mac-address*command to specify a MAC address to use or the **mac-address**use-virtual to use the MAC address range reserved for the VSS.

The MAC address range reserved for the VSS is derived from a reserved pool of addresses with the domain ID encoded in the leading 6 bits of the last octet and trailing 2 bits of the previous octet of the mac-address. The last two bits of the first octet is allocated for protocol mac-address which is derived by adding the protocol ID (0 to 3) to the router MAC address.

Note You must reload the virtual switch for the new router MAC address to take effect. If the MAC address you configured is different from the current MAC address, the following message is displayed: Configured Router mac address is different from operational value. Change will take effect after config is saved and switch is reloaded.

Examples

The following example shows how to specify the MAC address to use in hexadecimal format:

```
Router(config)# switch virtual domain test-mac-address
Router(config-vs-domain)# mac-address 0000.0000.0000
Router(config-vs-domain)#
```

The following example shows how to specify the MAC address range reserved for the VSS:

```
Router(config)# switch virtual domain test-mac-address
Router(config-vs-domain)# mac-address use-virtual
Router(config-vs-domain)#
```

Related Commands

Command	Description
switch virtual domain	Assigns a switch number and enters virtual switch domain configuration submode.

mac-address-table secure

To add secure addresses to the MAC address table, use the **mac-address-tablesecure** command in global configuration mode. To remove secure entries from the MAC address table, use the **no** form of this command.

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

no mac-address-table secure *hw-address* **vlan** *vlan-id*

Catalyst Switches

mac-address-table secure *hw-address* [**atm** *slot/port***vlan** *vlan-id*]
no mac-address-table secure *hw-address* [**vlan** *vlan-id*]

Cisco 860 Series Integrated Services Routers (ISRs) and Cisco 880 Series ISRs

mac-address-table secure [{**H . H . H** | **maximum** *maximum addresses*}]
no mac-address-table secure [{**H . H . H** | **maximum** *maximum addresses*}]

Syntax Description

hw -address	MAC address that is added to the table.
interface	Port to which packets destined for *hw-address* are forwarded.
fa	Specifies FastEthernet.
gi	Specifies Gigabit Ethernet.
H.H.H	(Optional) Specifies 48-bit hardware address.
slot	(Optional) The slot (slot 1 or slot 2) to which to add dynamic addresses.
port	(Optional) Port interface number. The ranges are based on type of Ethernet switch network module used: • 0 to 15 for NM-16ESW • 0 to 35 for NM-36ESW • 0 to 1 for GigabitEthernet
atm *slot* / *port*	(Optional) Add secure addresses to the ATM module in slot 1 or 2. The port is always 0 for an ATM interface.
maximum *maximum addresses*	(Optional) Applies only to Cisco 860 series and Cisco 880 series ISRs. Range is 1-200.

vlan *vlan -id*	Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers The *interface* and **vlan** parameters together specify a destination to which packets destined for *hw-address* are forwarded. The **vlan** keyword is optional if the port is a static-access VLAN port. In this case, the VLAN assigned to the port is assumed to be that of the port associated with the MAC address. This keyword is required for multi-VLAN and trunk ports. The value of *vlan-id* is the ID of the VLAN to which secure entries are added. Valid IDs are 1 to 1005; do not enter leading zeroes. Catalyst Switches (Optional) The *interface* and **vlan** parameters together specify a destination to which packets destined for *hw-address* are forwarded. The **vlan** keyword is optional if the port is a static-access VLAN port. In this case, the VLAN assigned to the port is assumed to be that of the port associated with the MAC address. This keyword is required for multi-VLAN and trunk ports. The value of *vlan-id* is the ID of the VLAN to which secure entries are added. Valid IDs are 1 to 1005; do not enter leading zeroes.

Command Default

Secure addresses are not added to the MAC address table.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2(8)SA	This command was introduced.
11.2(8)SA3	The **vlan** keyword was added.
11.2(8)SA5	The **atm** keyword was added.
12.2(2)XT	This command was implemented on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T, on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command with the **H.H.H** and **maximum** keyword was added for Cisco Series 860 ISRs and Cisco Series 880 ISRs.

Usage Guidelines

Cisco 860 Series ISRs, Cisco 880 Series ISRs, Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

Secure addresses can be assigned to only one port at a time. Therefore, if a secure address table entry for the specified MAC address and VLAN already exists on another port, it is removed from that port and assigned to the specified one.

If the maximum number is more than the MAC addresses statically specified by using the **H.H.H** keyword, the switch learns the MAC address automatically up to the specified maximum. If the maximum number is less than the number of MAC addresses already specified statically, then an error message displays.

Usage Guidelines

Catalyst Switches

Secure addresses can be assigned to only one port at a time. Therefore, if a secure address table entry for the specified MAC address and VLAN already exists on another port, it is removed from that port and assigned to the specified one.

Dynamic-access ports cannot be configured with secure addresses.

Cisco 860 Series ISRs, Cisco 880 Series ISRs

The following example shows how to allow ten devices on Fast Ethernet port 2:

```
Router(config)#
 mac-address-table secure maximum 10 ?
FastEthernet  FastEthernet IEEE 802.3
Router(config)#
 mac-address-table secure maximum 10 f ?
<0-4>  FastEthernet interface number
Router(config)#
mac-address-table secure maximum 10 f 2
```

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

The following example shows how to add a secure MAC address to VLAN 6 of port fa1/1:

Router(config)# mac-address-table secure 00c0.00a0.03fa fa1/1 vlan 6

Catalyst Switches

The following example shows how to add a secure MAC address to VLAN 6 of port fa1/1:

```
Switch(config)# mac-address-table secure 00c0.00a0.03fa fa1/1 vlan 6
```

The following example shows how to add a secure MAC address to ATM port 2/1:

```
Switch(config)# mac-address-table secure 00c0.00a0.03fa atm 2/1
```

Related Commands

Command	Description
clear mac -address-table	Deletes entries from the MAC address table.
mac -address-tableaging-time	Sets the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated.
mac -address-tabledynamic	Adds dynamic addresses to the MAC address table.

Command	Description
mac -address-tablestatic	Adds static addresses to the MAC address table.
show mac -address-table	Displays the MAC address table.

main-fiber port

To specify the port number to use for the optical link connection on the SDH/STM-1 trunk card on a Cisco AS5850, use the **main-fiberport** command in controller configuration mode.

main-fiber port {**0** | **1**}

Syntax Description

0	Specifies use of port 0 as the optical link connection. This is the default.
1	Specifies use of port 1 as the optical link connection.

Command Default

Port 0

Command Modes

Controller configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Use the**main-fiber** controller configuration command if you need to use optical port 1 during installation of the SDH/STM-1 trunk card on a Cisco AS5850 or if you suspect some problem with optical port 0.

This command does not have a **no** form. To restore the default value, use the **main-fiberport0**command.

Examples

The following example selects port 1 as the port with the optical connection:

```
Router(config)# controller sonet 1/0
Router(config-controller)# main-fiber port 1
```

max-reserved-bandwidth

To change the percent of interface bandwidth allocated for Resource Reservation Protocol (RSVP), class-based weighted fair queueing (CBWFQ), low latency queueing (LLQ), IP RTP Priority, Frame Relay IP RTP Priority, and Frame Relay PVC Interface Priority Queueing (PIPQ), use the **max-reservedbandwidth** command in interface configuration mode. To restore the default value, use the **no** form of this command.

max-reserved-bandwidth *percent*
no max-reserved-bandwidth

Syntax Description

percent	Percent of interface bandwidth allocated for RSVP, CBWFQ, LLQ, IP RTP Priority, Frame Relay IP RTP Priority, and Frame Relay PIPQ.

Command Default

75 percent on all supported platforms except the Cisco 7500 series routers, which do not have this restriction.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The sum of all bandwidth allocation on an interface should not exceed 75 percent of the available bandwidth on an interface. The remaining 25 percent of bandwidth is used for overhead, including Layer 2 overhead, control traffic, and best-effort traffic.

If you need to allocate more than 75 percent for RSVP, CBWFQ, LLQ, IP RTP Priority, Frame Relay IP RTP Priority, and Frame Relay PIPQ, you can use the **max-reserved-bandwidth** command. The *percent* argument specifies the maximum percentage of the total interface bandwidth that can be used.

If you do use the **max-reserved-bandwidth** command, make sure that not too much bandwidth is taken away from best-effort and control traffic.

Examples

In the following example, the policy map called policy1 is configured for three classes with a total of 8 Mbps configured bandwidth, as shown in the output from the **showpolicy-map** command:

```
Router# show policy-map policy1
 Policy Map policy1
  Weighted Fair Queueing
    Class class1
      Bandwidth 2500 (kbps) Max Threshold 64 (packets)
    Class class2
      Bandwidth 2500 (kbps) Max Threshold 64 (packets)
    Class class3
      Bandwidth 3000 (kbps) Max Threshold 64 (packets)
```

When you enter the **service-policy**command in an attempt to attach the policy map on a 10-Mbps Ethernet interface, an error message such as the following is produced:

```
I/f Ethernet1/1 class class3 requested bandwidth 3000 (kbps) Available only 2500 (kbps)
```

The error message is produced because the default maximum configurable bandwidth is 75 percent of the available interface bandwidth, which in this example is 7.5 Mbps. To change the maximum configurable bandwidth to 80 percent, use the **max-reserved-bandwidth** command in interface configuration mode, as follows:

```
max-reserved-bandwidth 80
service output policy1
end
```

To verify that the policy map was attached, enter the **showpolicy-mapinterface** command:

```
Router# show policy-map interface e1/1
 Ethernet1/1  output :policy1
  Weighted Fair Queueing
    Class class1
      Output Queue:Conversation 265
        Bandwidth 2500 (kbps) Packets Matched 0 Max Threshold 64 (packets)
        (discards/tail drops) 0/0
    Class class2
      Output Queue:Conversation 266
        Bandwidth 2500 (kbps) Packets Matched 0 Max Threshold 64 (packets)
        (discards/tail drops) 0/0
    Class class3
      Output Queue:Conversation 267
        Bandwidth 3000 (kbps) Packets Matched 0 Max Threshold 64 (packets)
        (discards/tail drops) 0/0
```

Virtual Template Configuration Example

The following example configures a strict priority queue in a virtual template configuration with CBWFQ. The **max-reserved-bandwidth** command changes the maximum bandwidth allocated between CBWFQ and IP RTP Priority from the default (75 percent) to 80 percent.

```
multilink virtual-template 1
interface virtual-template 1
 ip address 172.16.1.1 255.255.255.0
 no ip directed-broadcast
 ip rtp priority 16384 16383 25
 service-policy output policy1
 ppp multilink
 ppp multilink fragment-delay 20
 ppp multilink interleave
 max-reserved-bandwidth 80
 end
interface Serial0/1
 bandwidth 64
 ip address 10.1.1.2 255.255.255.0
 no ip directed-broadcast
 encapsulation ppp
 ppp multilink
 end
```

Note To make the virtual access interface function properly, do not configure the **bandwidth** command on the virtual template. Configure it on the actual interface, as shown in the example.

Related Commands

Command	Description
bandwidth (policy-map class)	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
ip rtp priority	Reserves a strict priority queue for a set of RTP packet flows belonging to a range of UDP destination ports.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
show policy-map	Displays the configuration of all classes comprising the specified service policy map or all classes for all existing policy maps.
show policy-map interface	Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface.

mdix auto

To enable automatic media-dependent interface with crossover detection, use the **mdixauto** command in interface configuration mode. To turn automatic detection off, use the **no** form of this command.

mdix auto
no mdix auto

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(17a)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported on all 10/100 and 10/100/1000 modules except for the following modules:

- WS-X6248-RJ45
- WS-X6248-TELCO
- WS-X6348-RJ-45
- WS-X6348-RJ-21
- WS-X6148-RJ-45
- WS-X6148-RJ-21

Examples

This example shows how to enable automatic media-dependent interface with crossover detection:

```
Router(config-if)# mdix auto
Router(config-if)
```

This example shows how to disable automatic media-dependent interface with crossover detection:

```
Router(config-if) no mdix auto
Router(config-if)
```

Related Commands

Command	Description
show interfaces	Displays the status and traffic statistics for the interfaces in the chassis.

mdl

To configure the Maintenance Data Link (MDL) message defined in the ANSI T1.107a-1990 specification, use the **mdl** command in controller configuration mode. To remove the message, use the **no** form of this command.

mdl {**transmit** {**path** | **idle-signal** | **test-signal**} | **string** {**eic** | **lic** | **fic** | **unit** | **pfi** | **port** | **generator**} *string*}
no mdl {**transmit** {**path** | **idle-signal** | **test-signal**} | **string** {**eic** | **lic** | **fic** | **unit** | **pfi** | **port** | **generator**} *string*}

Syntax Description

transmit path	Enables transmission of the MDL Path message.
transmit idle-signal	Enables transmission of the MDL Idle Signal message.
transmit test-signal	Enables transmission of the MDL Test Signal message.
string eic *string*	Specifies the Equipment Identification Code; can be up to 10 characters.
string lic *string*	Specifies the Location Identification Code; can be up to 11 characters.
string fic *string*	Specifies the Frame Identification Code; can be up to 10 characters.
string unit *string*	Specifies the Unit Identification Code; can be up to 6 characters.
string pfi *string*	Specifies the Path Facility Identification Code sent in the MDL Path message; can be up to 38 characters.
string port *string*	Specifies the Port number string sent in the MDL Idle Signal message; can be up to 38 characters.
string generator *string*	Specifies the Generator number string sent in the MDL Test Signal message; can be up to 38 characters.

Command Default

No MDL message is configured.

Command Modes

Controller configuration

Command History

Release	Modification
11.3	This command was introduced.
12.1(13)EX	This command was introduced on the Cisco 7304 router.
12.2(11)YT	This command was integrated into Cisco IOS Release 12.2(11)YT and implemented on the following platforms: Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3660 series, Cisco 3725, and Cisco 3745 routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was introduced on Cisco 7304 routers running Cisco IOS Release 12.2(18)S.

Release	Modification
12.2(25)S3	This command was integrated into Cisco IOS Release 12.2(25)S3 to support SPA on the Cisco 7304 routers.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE to support SPAs on the Cisco 7600 series routers and Catalyst 6500 series switches.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S to support SPAs on the Cisco 12000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the mdl command to send messages in maintenance data link in T3 c-bit framing mode.

Note MDL is supported only when the DS3 framing is C-bit parity.

Examples

The following example shows the **mdl** commands on a T3 controller in slot 1, port 0:

```
Router(config)# controller t3 1/0
Router(config-controller)# clock source line
Router(config-controller)# mdl string eic ID
Router(config-controller)# mdl string fic Building B
Router(config-controller)# mdl string unit ABC
Router(config-controller)# mdl string pfi Facility Z
Router(config-controller)# mdl string port Port 7
Router(config-controller)# mdl transmit path
Router(config-controller)# mdl transmit idle-signal
```

Related Commands

Command	Description
controller	Configures a T1, E1, or T3 controller and enters controller configuration mode.
show controllers serial	Displays serial line statistics.
show controllers t3	Displays information about T3 controllers.

media-type

To specify the physical connection on an interface, use the **media-type** command in interface configuration mode. To restore the default value, use the **no** form of this command.

media-type {**aui** | **10baset** | **100baset** | **mii** | **rj45** | **gbic**}
no media-type {**aui** | **10baset** | **100baset** | **mii**}

Syntax Description

aui	Selects an AUI 15-pin physical connection. This is the default on Cisco 4000 series routers.
10baset	Selects an R-J45 10BASE-T physical connection.
100baset	Specifies an RJ-45 100BASE-T physical connection. This is the default on Cisco 7000 series and Cisco 7200 series routers.
mii	Specifies a media-independent interface.
rj45	Specifies an RJ-45 physical connection. This is the default on Cisco 7304 series routers.
gbic	Specifies a Gigabit Interface Converter (GBIC) or small-form factor pluggable (SFP) physical connection for fiber media.

Command Default

An AUI 15-pin physical connection is the default setting on Cisco 4000 series routers. A 100BASE-T physical connection is the default setting on Cisco 7000 series and Cisco 7200 series routers. An RJ-45 physical connection is the default setting on Cisco 7304 series routers

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.1E	Support for Gigabit Ethernet was added with the **gbic** keyword.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(20)S2	This command was implemented on the 2-Port 10/100/1000 Gigabit Ethernet SPA on the Cisco 7304 router.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

To specify the physical connection on an interface, use the following interface configuration:

- Ethernet network interface module configuration on Cisco 4000 series routers
- Fast Ethernet Interface Processor (FEIP) on Cisco 7000 series, 7200 series, and 7500 series routers
- Full-duplex or half-duplex mode on a serial interface

Use the **media-type**interface configuration command to modify the default physical media connection type from **rj45** to **gbic** to configure a Gigabit Ethernet interface to support fiber media using a GBIC or SFP optical transceiver.

RJ-45 is the only media type supported by the 4-Port 10/100 Fast Ethernet SPA on the Cisco 7304 router, so the **media-type**command does not apply.

Examples

RJ-45 10BASE-T Example

The following example selects an RJ-45 10BASE-T physical connection on Ethernet interface 1:

```
Router(config)# interface ethernet 1
Router(config-if)# media-type 10baset
```

Fast Ethernet on a Cisco 7000 or Cisco 7200 Series Example

The following example specifies a media-independent interface physical connection to Fast Ethernet slot 0, port 1 on the Cisco 7000 or Cisco 7200 series:

```
Router(config)# interface fastethernet 0/1
Router(config-if)# media-type mii
```

Cisco 7500 Series Example

The following example specifies a media-independent interface physical connection to Fast Ethernet slot 0, port adapter 1, port 1 on the Cisco 7500 series:

```
Router(config)# interface fastethernet 0/1/1
Router(config-if)# media-type mii
```

Gigabit Ethernet with SPA on a Cisco 7304 Router Example

The following example configures the second interface (port 1) on a 2-Port 10/100/1000 Gigabit Ethernet SPA for a fiber SFP, where the SPA is installed in the bottom subslot (1) of the MSC, and the MSC is installed in slot 2 of the Cisco 7304 router:

Related Commands

Command	Description
show interfaces gigabitethernet	Displays information about the Gigabit Ethernet interfaces.

media-type auto-failover

To assign primary and secondary failover media on the GE-SFP port enter the **media-typeauto-failover** command in interface configuration mode. To automatically detect which media is connected, use the **no** form of this command.

media-type {**sfp** | **rj45**} **auto-failover**
no media-type

Syntax Description

sfp	Designates the SFP port as the primary media.
rj45	Designates the RJ45 port as the primary media
auto-failover	Configures the port with the primary media for automatic failover from SFP to RJ45 or vice-versa when the system goes down, reloads, and is unable to bring up primary media.

Command Default

No media-type. The primary media is not configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.0 (1) M	This command was introduced.

Examples

The following example shows how to configure the primary media as RJ45 and the secondary failover media as SFP:

```
Router(config-if)# media-type rj45 auto-failover
```

The following example shows how to configure the primary media as SFP and the secondary failover media as RJ45:

```
Router(config-if)# media-type sfp auto-failover
```

The following example shows how to configure the router to automatically detect which media is connected:

```
Router(config-if)# no media-type
```

Related Commands

Command	Description
media-type sfp	Specifies an SFP physical connection.
media-type rj45	Specifies an RJ-45 physical connection.

member subslot

To configure the redundancy role of a line card, use the member subslot command in line card redundancy group mode.

member subslot *slot/subslot* {**primary** | **secondary**}
no member subslot *slot/subslot* {**primary** | **secondary**}

Cisco uBR10012 Universal Broadband Routers

member subslot *slot/subslot* {
protect [**config** *slot/subslot* | **rf-power** [**rf-connector** *rfconnector-value*] {**hccp-delta** *diff-pwr* | **hccp-override** *override-pwr*}] | **working** [**rfsw-slot** *slot-value*] | **revertive** | **reverttime** *value*}

no member subslot *slot/subslot* {
protect [**config** *slot/subslot* | **rf-power** [**rf-connector** *rfconnector-value*] {**hccp-delta** *diff-pwr* | **hccp-override** *override-pwr*}] | **working** [**rfsw-slot** *slot-value*] | **revertive** | **reverttime** *value*}

Syntax Description

slot	Chassis line card slot number.
subslot	Chassis line card subslot number.
primary | **secondary**	Configures the redundancy role of the line card. • **primary** --Active line card. • **secondary** --Standby line card.
protect	Specifies the protect slot in the line card group.
config *slot/subslot*	(Optional) Specifies the appropriate working interface configuration that is used for the protect interface when a switchover occurs.
rf-power	(Optional) Specifies the RF power output level on an integrated upconverter.
rf-connector *rfconnector-value*	(Optional) Specifies the RF connector in the protect line card. The default value is all.
hccp-delta *diff-pwr*	When using N+1 Hotstandby Connection-to-Connection Protocol (HCCP) redundancy, the protect interface adds the diff-pwr value to the current power value of the working interface when a switchover occurs. This allows the router to accommodate relative differences between the RF power levels in working and protect interfaces. The valid value for diff-pwr ranges from –12 to +12 dBmV.

hccp-override *override-pwr*	When using N+1 HCCP redundancy, the protect interface uses the override power value instead of the power value of the working interface when a switchover occurs. This allows the router to accommodate absolute differences between the RF power levels in working and protect interfaces. The valid value for override-pwr ranges from 45 to 63 dBmV. **Note** The official range for acceptable power levels in the DOCSIS specification is 50 to 61 dBmV. Cisco cable interfaces exceed the DOCSIS standard, but power levels outside the DOCSIS standards should be used only in lab and test environments.
working	Specifies the working slot in the line card group.
rfsw-slot *slot-value*	(Optional) Specifies the RF switch slot for the working line card.
revertive	Specifies the revert operation on the protect card.
reverttime *value*	Specifies the time interval for the revert operation in minutes. If you specify the time interval as 30 minutes, the protect card switches back to the protect mode after 30 minutes.

Command Default

None

Command Modes

Line card redundancy group

Command History

Release	Modification
12.2(28)SB	This command was introduced on the Cisco 10000 series routers.
12.2(28)BC	This command was integrated into Cisco IOS Release 12.3(23)BC.
12.2(28)SCA	Support for the following keywords was removed in Cisco IOS Release 12.2(33)SCA and later releases: • **revertive** • **reverttime** **Note** Use the revertive command in line card redundancy group mode to enable the revert operation on a protect card in Cisco IOS Release 12.2(33)SCA and later releases.
12.2(28)SCC4	Support for the following keywords was added in Cisco IOS Release 12.2(33)SCC4 for Cisco uBR10012 routers: • **rf-power** • **rf-connector** • **hccp-delta** • **hccp-override**
12.2(28)SCE	The **config** option of the command was made the default. When more than one working line cards are configured, the config option is automatically applied to the first working card.

Usage Guidelines

The primary line card must be the first line card configured and must occupy subslot 1. The secondary line card must be the second line card configured and must occupy subslot 0. Only one primary line card and one secondary line card can be configured.

Note Configuration changes to the working line card cause the upstream links on the protect line card to flap. This is applicable only to Cisco uBR10012 routers.

Examples

The following example creates line card group number 1 for one-to-one line card redundancy. It also specifies the line card in subslot 1 as the primary (active) line card, and the line card in subslot 0 as the secondary (standby) line card:

```
Router(config)# redundancy
Router(config-red)# linecard-group 1 y-cable
Router(config-red-lc)# member subslot 2/1 primary
Router(config-red-lc)# member subslot 2/0 secondary
```

Note The rest of the examples listed here are only applicable to Cisco uBR10012 routers.

The following example shows how to configure a protect interface to add 3 dBmV to the current working RF power level when a switchover occurs:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# linecard-group 1 cable
Router(config-red-lc)# member subslot 5/1 protect rf-power hccp-delta 3
```

The following example shows how to configure a protect interface to use an RF power level of 48 dBmV instead of the current working RF power level when a switchover occurs:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# linecard-group 1 cable
Router(config-red-lc)# member subslot 5/1 protect rf-power hccp-override 48
```

The following example shows how to configure a rf-connector 3 on a protect interface to add 5 dBmV to the current working RF power level when a switchover occurs:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# linecard-group 1 cable
Router(config-red-lc)# member subslot 5/1 protect rf-power rf-connector 3 hccp-delta 5
```

Related Commands

Command	Description
linecard-group	Creates a line card group for one-to-one line card redundancy.

Command	Description
redundancy	Enters redundancy mode.
show redundancy linecard	Displays information about a redundant line card or line card group.

microcode reload controller

To reload the firmware and field programmable gate array (FPGA) without reloading the Cisco IOS image, use the **microcode reload controller** command in privileged EXEC mode.

microcode reload controller {**t1** | **e1** | **j1**} *x/y*

Syntax Description

t1	T1
e1	E1
j1	J1 controller.
x / *y*	Controller slot and unit numbers. The slash must be typed.

Command Default

No microcode reload activity is initiated.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(2)XH	This command was introduced on the Cisco 2600 series and Cisco 3600 series.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.2(8)T	The **j1** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Loopbacks in the running configuration are restored after this command is entered. If the controller is in a looped state before this command is issued, the looped condition is dropped. You have to reinitiate the loopbacks from the remote end by entering the **no loop**command from the controller configuration.

Examples

The following example shows how to start the microcode reload activity:

```
Router# microcode reload controller j1 3/0
TDM-connections and network traffic will be briefly disrupted.
Proceed with reload microcode?[confirm]
Router#
*Mar  3 209.165.200.225: clk_src_link_up_down: Status of this CLK does not matter
*Mar  3 209.165.200.226: clk_src_link_up_down: Status of this CLK does not matter
*Mar  3 209.165.200.227: %CONTROLLER-5-UPDOWN: Controller J1 3/0, changed state to)
*Mar  3 209.165.200.227: clk_src_link_up_down: Status of this CLK does not matter
*Mar  3 209.165.200.228: clk_src_link_up_down: Status of this CLK does not matter
*Mar  3 209.165.200.229: %CONTROLLER-5-UPDOWN: Controller J1 3/0, changed state top
*Mar  3 209.165.200.229: clk_src_link_up_down: Status of this CLK does not matter
*Mar  3 209.165.200.229: clk_src_link_up_down: Status of this CLK does not matter
```

mls exclude protocol

To specify the interface protocol to exclude from shortcutting, use the **mlsexcludeprotocol**command in global configuration mode. To remove a prior entry, use the **no** form of this command.

mls exclude protocol {**both** | **tcp** | **udp**} **port** *port-number*
no mls exclude

Syntax Description

both	Specifies both UDP and TCP.
tcp	Excludes TCP interfaces from shortcutting.
udp	Specifies UDP interfaces from shortcutting.
port *port-number*	Specifies the port number; valid values are from 1 to 65535.

Command Default

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to configure MLS to exclude UDP on port 69:

```
Router(config)#
mls exclude protocol udp port 69
Router(config)#
```

Related Commands

Command	Description
show mls ip multicast	Displays the MLS IP information.
show mls ipx	Displays MLS IPX information.

mls ip delete-threshold

To delete the configured access control list (ACL) thresholds, use the **mlsipdelete-threshold** comman d in global configuration mode.

mls ip delete-threshold *acl-num*

Syntax Description

acl-num	Reflective ACL number; valid values are from 1 to 10000.

Command Default

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

The **mlsipdelete-threshold** command is active only when you enable the **mlsipreflexivendr-entrytcam** command.

Examples

This example shows how to delete an ACL threshold:

```
Router(config)# mls ip delete-threshold 223
Router(config)#
```

Related Commands

Command	Description
mls ip install-threshold	Installs the configured ACL thresholds.
mls ip reflexive ndr-entry tcam	Enables the shortcuts in TCAM for the reflexive TCP/UDP entries when installed by the NDR.

mls ip directed-broadcast

To enable the hardware switching of the IP-directed broadcasts, use the **mlsipdirected-broadcast** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

mls ip directed-broadcast {**exclude-router** | **include-router**}
no mls ip directed-broadcast

Syntax Description

exclude-router	Forwards the IP-directed broadcast packet in the hardware to all hosts in the VLAN except the router.
include-router	Forwards the IP-directed broadcast packet in the hardware to all hosts in the VLAN including the router.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **exclude-router** and **include-router** keywords both support hardware switching, but **exclude-router** does not send a copy of the hardware-switched packets to the router. If you enter the **include-router** keyword, the router does not forward the IP-directed broadcast packet again.

In the default mode, IP-directed broadcast packets are not hardware forwarded; they are handled at the process level by the MSFC. The MSFC decision to forward or not forward the packet is dependent on the **ipdirected-broadcast** command configuration.

There is no interaction between the **ipdirected-broadcast** command and the **mlsipdirected-broadcast** command. The **ipdirected-broadcast** command involves software forwarding, and the **mlsipdirected-broadcast** command involves hardware forwarding.

MLS IP-directed broadcast supports a secondary interface address.

Any packets that hit the CPU are not forwarded unless you add the **ipdirected-broadcast** command to the same interface.

You can configure the MLS IP-directed broadcasts on a port-channel interface but not on the physical interfaces on the port-channel interface. If you want to add a physical interface to a port-channel group, the physical interface cannot have the MLS IP-directed broadcast configuration. You have to first remove the configuration manually and then add the physical interface to the channel group. If a physical interface is already part of a channel group, the CLI will not accept the **mlsipdirected-broadcast** configuration command on that physical interface.

Examples

This example shows how to forward the IP-directed broadcast packet in the hardware to all hosts in the VLAN with the exception of the router:

```
Router(config-if)#
mls ip directed-broadcast exclude-router
Router(config-if)#
```

This example shows how to forward the IP-directed broadcast packet in the hardware to all hosts in the VLAN:

```
Router(config-if)#
mls ip directed-broadcast include-router
Router(config-if)#
```

Related Commands

Command	Description
show mls cef adjacency	Displays information about the MLS-hardware Layer 3-switching adjacency node.

mls ipx

To enable Multilayer Switching (MLS) Internetwork Packet Exchange (IPX) on the interface, use the **mlsipx**command in interface configuration mode. To disable IPX on the interface, use the **no** form of this command.

mls ipx
no mls ipx

Syntax Description

This command has no arguments or keywords.

Command Default

Multicast is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720.

Examples

This example shows how to enable MLS IPX on an interface:

```
Router(config-if)#
mls ipx
Router(config-if)#
```

Related Commands

Command	Description
mls rp ipx (interface configuration mode)	Allows the external systems to enable MLS IPX on the interface.
show mls ipx	Displays MLS IPX information.

mls verify

To enable Layer 3 error checking in the hardware, use the **mlsverify** command in global configuration mode. To disable Layer 3 error checking in the hardware, use the **no** form of this command.

mls verify {**ip** | **ipx**} {**checksum** | **length** {**consistent** | **minimum**}}
no mls verify {**ip** | **ipx**} {**checksum** | **length** {**consistent** | **minimum**}}

Syntax Description

ip	Specifies the IP-checksum errors.
ipx	Specifies the IPX checksum errors.
checksum	Enables the checksum-error check.
length consistent	Enables the length-consistency check in Layer 2.
length minimum	Enables the minimum-length packet check in Layer 2.
consistent	Specifies the length-consistency check in Layer 2.
minimum	Enables the minimum-length packet check in Layer 2.

Command Default

checksum

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	This command was changed to include the **minimum** keyword on the Supervisor Engine 720. Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The minimum-length packets are the packets with an IP header length or IP total length field that is smaller than 20 bytes.

When entering the minimum keyword, follow these guidelines:

- When enabling the IP "too short" check using the mls verify ip length minimum command, valid IP packets with with an IP protocol field of ICMP(1), IGMP(2), IP(4), TCP(6), UDP(17), IPv6(41), GRE(47), or SIPP-ESP(50) will be hardware switched. All other IP protocol fields are software switched.

Caution Using optimized access-list logging (OAL) and the mls verify ip length minimum command together can cause routing protocol neighbor flapping as they are incompatible

- When entering the **nomlsverifyiplengthminimum** command, minimum-length packets are hardware switched. The packets that have IP protocol = 6 (TCP) are sent to the software.

Examples

This example shows how to enable Layer 3 error checking in the hardware:

```
Router(config
)# mls verify ip checksum
Router(config)#
```

This example shows how to disable Layer 3 error checking in the hardware:

```
Router(config
)# no mls verify ip checksum
Router(config)#
```

mobility

To configure the wireless mGRE tunnels, use the **mobility** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

mobility {**network-id** *id* | **tcp** **adjust-mss**}
mobility [{**trust** | **broadcast**}]

Syntax Description

network-id *id*	Specifies the wireless network ID for the mGRE tunnel; valid values are from 1 to 4095.
tcp adjust-mss	Adjusts the MSS value in TCP SYN and TCP ACK on the access points automatically.
trust	(Optional) Specifies the trusted network.
broadcast	(Optional) Specifies that the mGRE tunnel convert the NBMA to the BMA.

Command Default

Untrusted network

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 720.
12.2(18)SXD3	This command was changed to include the **tcpadjust-mss** keywords.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported on Cisco 7600 series routers that are configured with a WLSM only.

The **tcpadjust-mss** keywords are supported on mGRE tunnel interfaces only.

You can enter the **iptcpadjust-mss***value* command to change the TCP MSS to a lower value.

A trusted network can use DHCP or a static IP address. An untrusted network supports only DHCP clients.

Examples

This example shows how to specify the network identification number for the mGRE tunnel:

```
Router(config-if)# mobility network-id 200
Router(config-if)#
```

This example shows how to specify the trusted network:

```
Router(config-if)# mobility trust
Router(config-if)#
```

This example shows how to specify that the mGRE tunnel convert the NBMA to the BMA:

```
Router(config-if)# mobility broadcast
Router(config-if)#
```

This example shows how to adjust the MSS value in TCP SYN and TCP ACK on the access points automatically:

```
Router(config-if)# mobility tcp adjust-mss
Router(config-if)#
```

Related Commands

Command	Description
ip tcp adjust-mss	Adjusts the MSS value of TCP SYN packets going through a router.
show mobility	Displays information about the Layer 3 mobility and the wireless network.

mode

To set the redundancy mode, use the **mode** command in redundancy configuration mode.

Syntax for 12.2S Release
mode {**rpr** | **rpr-plus** | **sso**}

Syntax for Cisco IOS XE Release 2.5 and Later Releases
mode {**rpr** | **sso**}

Syntax for 12.2XNE Release
mode **sso**

Syntax Description

rpr	Specifies Route Processor Redundancy (RPR) mode.
rpr-plus	Specifies Route Processor Redundancy Plus (RPR+) mode.
sso	Specifies stateful switchover (SSO) mode.

Command Default

- The default is SSO mode if the system is not configured for redundancy and the active and standby supervisor engines have the same image.
- The default is RPR mode if different versions are installed.
- If redundancy is enabled, the default is the mode that you have configured.

- The default is RPR+ mode if the system is not configured for redundancy and the active and standby supervisor engines have the same image.
- The default is RPR mode if different versions are installed.
- If redundancy is enabled, the default is the mode that you have configured.

- The default is SSO mode if the system is not configured for redundancy and the active and standby supervisor engines have the same image.
- The default is RPR mode if different versions are installed.

- The default is SSO mode if the system is not configured for redundancy and the active and standby supervisor engines have the same image.
- The default is RPR mode if different versions are installed.

Command Modes

Redundancy configuration (config-red)

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17b)SXA	This command was modified. Support was added for SSO mode and the default mode change.

Release	Modification
12.2(17d)SXB	This command was modified. Support was added for multicast and unicast traffic.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)XNE	This command was modified. This command was implemented on the Cisco 10000 router.
Cisco IOS XE Release 2.5	This command was modified. This command was implemented on the Cisco ASR 1000 Series Routers.

Usage Guidelines

Cisco IOS Release 12.2S and 7600 Series Routers

SSO is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

On releases prior to Release 12.2(17d)SXB, single router mode (SRM) with SSO redundancy does not support stateful switchover for multicast traffic. When a switchover occurs, all multicast hardware switching entries are removed and are then re-created and reinstalled in the hardware by the newly active multilayer switch feature card (MSFC).

SRM/SSO is supported in the following releases only:

- Release 12.2(17b)SXA and subsequent rebuilds.
- Release 12.2(17d)SXB and subsequent rebuilds.

Nonstop forwarding (NSF) with SSO redundancy mode supports IPv4. NSF with SSO redundancy mode does not support IPv6, Internetwork Packet Exchange (IPX), and Multiprotocol Label Switching (MPLS).

If you have configured MPLS on the Cisco 7600 series routers with redundant supervisor engines, you must configure the Cisco 7600 series router in RPR mode. The switch should not be running in the default mode of SSO.

Enter the **redundancy** command in global configuration mode to enter redundancy configuration mode. You can enter the **mode** command within redundancy configuration mode.

Follow these guidelines when configuring your system for RPR+ mode:

- You must install compatible images on the active and standby supervisor engines to support RPR+ mode and SSO mode.
- Both supervisor engines must run the same Cisco IOS software version.
- Any modules that are not online at the time of a switchover are reset and reloaded on a switchover.
- The Forwarding Information Base (FIB) tables are cleared on a switchover. As a result, routed traffic is interrupted until route tables reconverge.

The standby supervisor engine reloads on any change of mode and begins to work in the current mode. When you use this command to force the standby supervisor engine to run as a Distributed Forwarding Card (DFC) card, the uplink ports in the standby engine continue to be in use and are not disabled.

Cisco IOS Release XE Release 2.5 and ASR 1000 Series Routers

For Cisco ASR 1002 and 1004 routers, RRP and stateful switchover can be used to switch between Cisco IOS processes. RPR and SSO need to be configured by the user, however, because a second Cisco IOS process is not available by default on Cisco ASR 1002 and 1004 routers. Enter the **redundancy** command in global configuration mode to enter redundancy configuration mode. You can enter the **mode** command within redundancy configuration mode.

The Cisco ASR 1006 Router supports a second Route Processor. The second Cisco IOS process can run only on the standby Route Processor. This means that hardware redundancy is available and RPR and SSO do not need to be configured by the user because a second Cisco IOS process is available by default on the Cisco ASR 1006 router.

RPR+ mode is not supported on the Cisco ASR 1000 Series Routers.

Cisco IOS Release 12.2XNE and 1000 Series Routers

Enter the **redundancy** command in global configuration mode to enter redundancy configuration mode. You can enter the **mode** command within redundancy configuration mode.

RPR mode is not supported on the Cisco 10000 router.

Examples

This example shows how to set the redundancy mode to RPR+:

```
Router(config)# redundancy
Router(config-red)# mode rpr-plus
```

This example shows how to set the redundancy mode to SSO:

```
Router(config)# redundancy
Router(config-red)# mode sso
```

Related Commands

Command	Description
redundancy	Enters redundancy configuration mode.
redundancy force-switchover	Forces a switchover from the active to the standby supervisor engine.
route-converge-interval	Configures the time interval after which the old FIB entries are purged.
show redundancy	Displays RF information.
show running-config	Displays the status and configuration of the module or Layer 2 VLAN.

mode (ATM T1 E1 controller)

To set the DSL controller into ATM mode and create an ATM interface or to set the T1 or E1 controller into T1 or E1 mode and create a logical T1/E1 controller, use the **mode** command in controller configuration mode. To disable the current mode and prepare to change modes, use the **no** form of this command.

Cisco 1800, Cisco 2800, Cisco 3700, Cisco 3800 Series
mode atm
no mode atm

Cisco 1700 Series, Cisco 2600XM
mode {**atm** | **t1** | **e1**}
no mode {**atm** | **t1** | **e1**}

Cisco IAD2430
mode {**atm** [**aim** *aim-slot*] | **cas** | **t1** | **e1**}
no mode {**atm** [**aim** *aim-slot*] | **cas** | **t1** | **e1**}

Syntax Description

atm	Sets the controller into ATM mode and creates an ATM interface (ATM 0). When ATM mode is enabled, no channel groups, DS0 groups, PRI groups, or time-division multiplexing (TDM) groups are allowed, because ATM occupies all the DS0s on the T1/E1 trunk. When you set the controller to ATM mode, the controller framing is automatically set to extended super frame (ESF) for T1 or cyclic redundancy check type 4 (CRC4) for E1. The line code is automatically set to binary 8-zero substitution (B8ZS) for T1 or high-density bipolar C (HDBC) for E1. When you remove ATM mode by entering the **nomodeatm** command, ATM interface 0 is deleted. **Note** The **modeatm** command without the **aim** keyword uses software to perform ATM segmentation and reassembly (SAR). This is supported on Cisco 2600 series WIC slots only; it is not supported on network module slots.
aim	(Optional) The configuration on this controller uses the Advanced Integration Module (AIM) in the specified slot for ATM SAR. The **aim** keyword does not apply to the Cisco IAD2430 series IAD.
aim-slot	(Optional) AIM slot number on the router chassis: • Cisco 2600 series--0. • Cisco 3660--0 or 1.
cas	(Cisco 2600 series WIC slots only) Channel-associated signaling (CAS) mode. The T1 or E1 in this WIC slot is mapped to support T1 or E1 voice (that is, it is configured in a DS0 group or a PRI group). CAS mode is supported on both controller 0 and controller 1. On the Cisco IAD2430 series IAD, CAS mode is not supported.

t1	Sets the controller into T1 mode and creates a T1 interface. When you set the controller to T1 mode, the controller framing is automatically set to ESF for T1. The line code is automatically set to B8ZS for T1.
e1	Sets the controller into E1 mode and creates an E1 interface. When you set the controller to E1 mode, the controller framing is automatically set to CRC4 for E1. The line code is automatically set to HDB3 for E1.

Command Default

The controller mode is disabled.

Command Modes

Controller configuration

Command History

Release	Modification
11.3 MA	This command was introduced on the Cisco MC3810.
12.1(5)XM	Support for this command was extended to the merged SGCP/MGCP software.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T for the Cisco IAD2420.
12.2(2)XB	Support was extended to the Cisco 2600 series and Cisco 3660. The keyword **aim** and the argument *aim-slot* were added. The parenthetical modifier for the command was changed from “Voice over ATM” to “T1/E1 controller.”
12.2(15)T	This command was implemented on the Cisco 2691 and the Cisco 3700 series.
12.3(4)XD	This command was integrated into Cisco IOS Release 12.3(4)XD on Cisco 2600 series and Cisco 3700 series routers to configure DSL Frame mode and to add T1/E1 Framed support.
12.3(4)XG	This command was integrated into Cisco IOS Release 12.3(4)XG on the Cisco 1700 series routers.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T on Cisco 2600 series and Cisco 3700 series routers.
12.3(11)T	This command was implemented on Cisco 2800 and Cisco 3800 series routers.
12.3(14)T	This command was implemented on Cisco 1800 series routers.

Usage Guidelines

When a DSL controller is configured in ATM mode, the mode must be configured identically on both the CO and CPE sides. Both sides must be set to ATM mode.

Note If using the **nomodeatm** command to leave ATM mode, the router must be rebooted immediately to clear the mode.

When configuring a DSL controller in T1 or E1 mode, the mode must be configured identically on the CPE and CO sides.

Examples

ATM Mode Example

The following example configures ATM mode on the DSL controller.

```
Router(config)# controller
 dsl
 3/0
Router(config-controller)# mode atm
```

T1 Mode Example

The following example configures T1 mode on the DSL controller.

```
Router(config)# controller
 dsl
 3/0
Router(config-controller)# mode t1
```

Related Commands

Command	Description
channel-group	Configures a list of time slots for voice channels on controller T1 0 or E1 0.
tdm-group	Configures a list of time slots for creating clear channel groups (pass-through) for time-division multiplexing (TDM) cross-connect.

mode (HSA redundancy)

To configure the redundancy mode, use the **mode**command in redundancy configuration mode. To configure the default redundancy mode, use the **no**form of this command.

mode {**hsa** | **rpr** | **rpr-plus**}
no **mode** {**hsa** | **rpr** | **rpr-plus**}

Syntax Description

hsa	Selects High System Availability (HSA) redundancy mode. This is the default.
rpr	Selects Route Processor Redundancy (RPR) mode.
rpr-plus	Selects Route Processor Redundancy Plus (RPR+) redundancy mode.

Command Default

HSA redundancy mode

Command Modes

Redundancy configuration

Command History

Release	Modification
12.0(16)ST	This command was introduced.
12.0(19)ST1	The **rpr-plus**keyword was added.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines

The mode selected by the **mode** command in redundancy configuration mode must be fully supported by the image that has been installed in both the active and standby Route Switch Processors (RSPs). A high availability image must be installed in the RSPs before RPR+ can be configured. Use the**hw-moduleslotimage**command to specify a high availability image to run on the standby RSP.

If the mode cannot be set on both RSPs, HSA is the default mode. A Cisco 7507 or Cisco 7513 router that has only one RSP installed operates in single Route Processor mode.

Examples

The following example enters redundancy configuration mode and sets RPR+ as the redundancy mode for a Cisco 7500 series router.

```
Router(config)# redundancy
Router(config-r)# mode rpr-plus
Router(config-r)# end
```

Related Commands

Command	Description
hw-module sec-cpu reset	Resets and reloads the standby RSP with the specified Cisco IOS image and executes the image.

Command	Description
hw-module slot image	Specifies a high availability Cisco IOS image to run on an active or standby RSP.
redundancy	Enters redundancy configuration mode.
redundancy force-switchover	Switches control of a router from the active RSP to the standby RSP.
show redundancy	Displays the current redundancy mode.

mode (RSC redundancy)

To choose between classic-split mode (maximum throughput with no load sharing) and handover-split mode (maximum availability with load sharing), use the **mode** command in redundancy configuration mode. To reset to the default mode, use the **no** form of this command.

mode {**classic-split** | **handover-split**}
no mode

Syntax Description

classic-split	Nonredundant mode in which slots are split in a fixed 6/6 pattern between the two route-switch-controller (RSC) cards, and no handover occurs. This is the default.
handover-split	Redundant mode in which, if one RSC fails, the peer RSC takes over control of the failed RSC's resources (slots and cards).

Command Default

Classic-split mode

Command Modes

Redundancy configuration

Command History

Release	Modification
12.2(2)XB1	This command was introduced.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

You must be connected to an RSC card on your Cisco AS5850 to use this command.

Examples

The following example selects handover-split mode:

```
Router(config)# redundancy
Router(config-r)#

mode handover-split
```

Related Commands

Command	Description
show chassis	Displays, for a router with two RSCs, information about mode (handover-split or classic-split), RSC configuration, and slot ownership.
show chassis clocks	Displays all configured clock sources, even those from non-owned cards. This is because only one RSC can provide the master clock, and it may need to have backup clock sources configured from all cards present, regardless of ownership.
show context	Displays information about specified slots.
show redundancy debug-log	Displays up to 256 redundancy-related debug entries.

mode (T1 E1 controller)

To set the T1 or E1 controller into asynchronous transfer mode (ATM) and create an ATM interface, to set the T1 or E1 controller into T1 or E1 mode and create a logical T1 or E1 controller, or to set the T1 or E1 controller into channel-associated signaling (CAS) mode, use the **mode** command in controller configuration mode. To disable the current mode and prepare to change modes, use the **no**form of this command.

mode {**atm** [**aim** *aim-slot*] | **cas** | **t1** | **e1**}
no mode {**atm** [**aim** *aim-slot*] | **cas** | **t1** | **e1**}

Syntax Description

atm	Sets the controller into ATM mode and creates an ATM interface (ATM 0). When ATM mode is enabled, no channel groups, DS0 groups, PRI groups, or time-division multiplexing (TDM) groups are allowed, because ATM occupies all the DS0s on the T1/E1 trunk. When you set the controller to ATM mode, the controller framing is automatically set to extended super frame (ESF) for T1 or cyclic redundancy check type 4 (CRC4) for E1. The line code is automatically set to binary 8-zero substitution (B8ZS) for T1 or high-density bipolar C (HDB3) for E1. When you remove ATM mode by entering the **no mode atm** command, ATM interface 0 is deleted. On the Cisco MC3810, ATM mode is supported only on controller 0 (T1 or E1 0). **Note** The **mode atm** command without the **aim** keyword uses software to perform ATM segmentation and reassembly (SAR). This is supported on Cisco 2600 series WIC slots only and is not supported on network module slots.
aim	(Optional) The configuration on this controller uses the Advanced Integration Module (AIM) in the specified slot for ATM SAR. The **aim** keyword does not apply to the Cisco MC3810 and the Cisco IAD2420 series IAD.
aim-slot	(Optional) AIM slot number on the router chassis. For the Cisco 2600 series, the AIM slot number is 0; for the Cisco 3660, the AIM slot number is 0 or 1.
cas	(CAS mode on Cisco 2600 series WIC slots only) The T1 or E1 in this WIC slot is mapped to support T1 or E1 voice (it is configured in a DS0 group or a PRI group). CAS mode is supported on both controller 0 and controller 1.
t1	(Cisco 2600XM series using the G.SHDSL WIC only) Sets the controller into T1 mode and creates a T1 interface. When you set the controller to T1 mode, the controller framing is automatically set to ESF for T1. The line code is automatically set to B8ZS for T1.
e1	(Cisco 2600XM series using the G.SHDSL WIC only) Sets the controller into E1 mode and creates an E1 interface. When you set the controller to E1 mode, the controller framing is automatically set to CRC4 for E1. The line code is automatically set to HDB3 for E1.

Command Default

No controller mode is configured.

Command Modes

Controller configuration

Command History

Release	Modification
11.3 MA	This command was introduced on the Cisco MC3810.
12.1(5)XM	Support for this command was extended to Simple Gateway Control Protocol (SGCP) and Media Gateway Control Protocol (MGCP).
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series.
12.2(2)XB	Support was extended to the Cisco 2600 series and Cisco 3660. The **aim**keyword and the *aim-slot* argument were added. The parenthetical modifier for the command was changed from "Voice over ATM" to "T1/E1 controller."
12.2(8)T	This command was implemented on the Cisco IAD2420 series.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.
12.2(15)T	This command was implemented on the Cisco 2691 and the Cisco 3700 series.
12.3(4)XD	Support was extended on Cisco 2600 series and Cisco 3700 series routers to configure DSL Frame mode and to add T1/E1 Framed support.
12.3(7)T	The support that was added in Cisco IOS Release 12.3(4)XD was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

This command has the following platform-specific usage guidelines:

- Cisco 2600 series, Cisco 3660 routers, or Cisco 3700 series that use an AIM for ATM processing must use the **mode atm aim***aim-slot* command.
- Cisco 2600 series routers that use an AIM for DSP processing and specify DS0 groups must use the **mode cas** command if they are using WIC slots for voice. This command does not apply if network modules are being used.
- Cisco 3660 routers or Cisco 3700 series that use an AIM only for DSP resources should not use this command.
- On Cisco 2600 series routers that use WIC slots for voice, the **mode atm** command without the **aim** keyword specifies software ATM segmentation and reassembly. When the **aim** keyword is used with the **mode atm** command, the AIM performs ATM segmentation and reassembly.
- Cisco MC3810 routers cannot use the **aim** keyword.
- Cisco MC3810 routers with digital voice modules (DVMs) use some DS0s exclusively for different signaling modes. The DS0 channels have the following limitations when mixing different applications (such as voice and data) on the same network trunk:
  - On E1 controllers, DS0 16 is used exclusively for either CAS or common channel signaling (CCS), depending on which mode is configured.
  - On T1 controllers, DS0 24 is used exclusively for CCS.

- Cisco MC3810--When no mode is selected, channel groups and clear channels (data mode) can be created using the **channel group** and **tdm-group** commands, respectively.
- Cisco MC3810 is not supported in the AIM-ATM, AIM-VOICE-30, and AIM-ATM-VOICE-30 on the Cisco 2600 Series, Cisco 3660, and Cisco 3700 Series feature.
- On Cisco 2600 series and Cisco 3700 series routers when configuring a DSL controller in ATM mode, the mode must be set to the same mode on both the CO and CPE sides. Both sides must be set to ATM mode.
    - If the **no mode atm** command is used to leave ATM mode, the router must be rebooted immediately to clear the mode.
- On Cisco 2600 series and Cisco 3700 series routers when configuring a DSL controller in T1 or E1 mode, the mode must be configured identically on the CO and CPE sides.

Examples

The following example configures ATM mode on controller T1 0. This step is required for Voice over ATM.

```
Router(config)# controller
 T1 0
Router(config-controller)# mode atm
```

The following example configures ATM mode on controller T1 1/ 0 on a Cisco 2600 series router using an AIM in slot 0 for ATM segmentation and reassembly:

```
Router(config)# controller
 t1 1/0
Router(config-controller)# mode atm aim 0
```

The following example configures CAS mode on controller T1 1 on a Cisco 2600 series router:

```
Router(config)# controller
 T1 1
Router(config-controller)# mode cas
```

The following example configures ATM mode on the DSL controller.

```
Router(config)# controller
 dsl 3/0
Router(config-controller)# mode atm
```

The following example configures T1 mode on the DSL controller.

```
Router(config)# controller
 dsl
 3/0
Router(config-controller)# mode t1
```

Related Commands

Command	Description
channel-group	Defines the time slots for voice channels on controller T1 0 or E1 0.
tdm-group	Configures a list of time slots for creating clear channel groups (pass-through) for TDM cross-connect.

mode bypass

To enable Virtual Multipoint Interfaces (VMI) to support multicast traffic, use the **modebypass** command in interface configuration mode. To return the interface to the default mode of aggregate, use the **no** form of this command.

mode [{**aggregate** | **bypass**}]
no mode bypass

Syntax Description

aggregate	Sets the mode to aggregate. All virtual-access interfaces created by PPPoE sessions are logically aggregated under the VMI.
bypass	Sets the mode to bypass.

Command Default

No mode

Command Modes

Interface configuration

Command History

Release	Modification
12.4(15)XF	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T to support multicast traffic on Virtual Multipoint Interfaces (VMIs).

Usage Guidelines

Use the mode bypass command when you need to support multicast traffic in router-to-radio configurations.

Aggregate Mode

The default mode for operation of the VMI is **aggregate** mode. In aggregate mode, all of the virtual-access interfaces created by PPPoE sessions are logically aggregated under the VMI. As such, applications above Layer 2, such as, EIGRP and OSPFv3, should be defined on the VMI interface only. Packets sent to the VMI will be correctly forwarded to the correct virtual-access interface.

Bypass Mode

Using **bypass** mode is recommended for multicast applications.

In **bypass** mode, the virtual-access interfaces are directly exposed to applications running above Layer2. In bypass mode, definition of a VMI is still required because the VMI will continue to manage presentation of cross-layer signals, such as, neighbor up, neighbor down, and metrics. However, applications will still be aware on the actual underlying virtual-access interfaces and send packets to them directly.

Using **bypass** mode can cause databases in the applications to be larger because knowledge of more interfaces are required for normal operation.

After you enter the **modebypass** command, Cisco recommends that you copy the running configuration to NVRAM. because the default mode of operation for VMI is to logically aggregate the virtual-access interfaces.

Examples

The following example sets the interface mode to bypass:

```
Router# enable
Router# configure terminal
Router(config)# interface vmi1
Router(config-if)# mode bypass
```

Related Commands

Command	Description
interface vmi	Creates a VMI interface.

mode c-12

To configure the mode of an E1 line that has been mapped to a TUG-3, use the mode c-12 command in configuration controller tug3 mode.To configure the mode of an E1 line that has been mapped to a AU-3, use the mode c-12 command in configuration controller au3 mode. To disable the mode configuration, use the **no** form of this command.

mode c-12
no mode c-12m

Syntax Description

This command has no arguments or keywords

Command Default

Disabled

Command Modes

Configuration controller tug3 (for an E1 line mapped to a TUG-3) Configuration controller au3 (for an E1 line mapped to an AU-3)

Command History

Release	Modification
12.0(14)S	This command was introduced.
12.1(7)E	This command was integrated into Cisco IOS Release 12.1(7)E, and support was added for Cisco 7200 VXR routers and Catalyst 6000 family switches.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can configure each of the TUG-3s or AU-3s of a PA-MC-STM-1 to carry a set of TU-12s (E1s mapped into TU-12s). The **modec-12**command configures the mode of operation of a TUG-3 or AU-3 and specifies that the TUG-3 or AU-3 is divided into 21 TU-12s, each carrying an E1.

Examples

The following example configures the AUG-mapping of the SONET controller to AU-3 and specifies the mode of AU-3 1 to c-12 on a Cisco 7500 series router:

```
Router(config)# controller sonet 1/0/0
Router(config-controller)# aug mapping au-3
Router(config-controller)# au3 1
Router(config-ctrlr-au3)# mode c-12
```

The following example configures the AUG-mapping of the SONET controller to AU-4 and specifies the mode of TUG-3 1 of AU-4 1 to c-12 on a Cisco 7200 VXR router or a Catalyst 6000 family switch:

```
Router(config)# controller sonet 1/0
```

```
Router(config-controller)# aug mapping au-4
Router(config-controller)# au-4 1 tug-3 1
Router(config-ctrlr-tug3)# mode c-12
```

mode ct3

Use this command to configure channelized T3 mode.

mode ct3

Syntax Description

Syntax Description:

There are no keywords for this command.

Command Default

None

Command Modes

Controller configuration

Command History

Release	Modification
XE 3.18 SP	Support for this command was introduced on NCS 4200 Series.

Examples

The following example shows how to configure DS1 CT3 SAToP mode:

```
Router> enable
Router#configure terminal
Router(config)# controller MediaType 0/5/0
Router(config-ctr)# mode sonet
Router(config-ctr-sonet)# controller sonet 0/5/0
Router(config-ctr-sonet)# rate oc12
Router(config-ctr-sonet)# sts-1 1
Router(config-ctr-sonet)# mode ct3
Router(config-ctr-sonet)# t1 1 cem-group 100 unframed
Router(config-ctr-sonet)# t1 1 framing unframed
Router(config)# interface cem 0/5/0
Router(config-if)#cem 100
Router(config-if)#xconnect 2.2.2.2 10 encapsulation mpls
Router(config-if)#end
```

Related Commands

Command	Description
controller sonet	Configures the SONET mode.
show controller sonet	Displays SONET controller configuration.
show controller t3	Displays T3 controller configuration.

mode download

To enable operational code download mode for the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT), use the **modedownload**command in satellite initial configuration mode. To disable operational code download mode, use the **no** form of this command.

mode download
no mode download

Syntax Description

This command has no arguments or keywords.

Command Default

Operational code download mode is enabled.

Command Modes

Satellite initial configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

This command is typically used by an installation technician. Do not use this command unless your satellite service provider instructs you to perform the satellite initial configuration and provides all necessary parameter values.

Examples

The following example shows how to disable operational code download mode:

```
Router(sat-init-config)# no mode download
```

mode e3

Use this command to configure E3 mode.

mode e3

Syntax Description

Syntax Description

None

Command Default

None

Command Modes

Controller configuration

Command History

Release	Modification
XE Everest 16.6.1	This command was integrated into the Cisco NCS 4200 Series and Cisco ASR 900 Series.

Usage Guidelines

You can change the mode of a controller only when there are no subinterfaces defined for the controller.

Examples

```
enable
configure terminal
controller sdh 0/5/0
rate stm4
au-4 1
mode tug-3
tug-3 1
mode e3
cem-group 100 unframed
end
```

Related Commands

Command	Description
show running configuration	Verifies mode E3 configuration.

mode sonet

Use this command to configure SONET controller configuration mode.

mode sonet

Syntax Description

Syntax Description:

This command has no arguments or keywords.

Command Default

This command is disabled by default; no AIS is sent.

Command Modes

Controller configuration

Command History

Release	Modification
XE 3.18 SP	Support for this command was introduced on NCS 4200 Series.

Usage Guidelines

This command is used to configure the SONET controller mode.

Examples

The following example shows how to configure SONET mode:

```
enable
configure terminal
controller MediaType 0/5/0
mode sonet
end
```

Related Commands

Command	Description
controller mediatype	Configures the mediatype controller.
controller sonet	Displays information about Synchronous Optical Network (SONET) controllers.
show controller sonet	Displays SONET controller configuration.

mode sts-nc

To configure the concatenated signals in the SONET network, use the **mode** *sts-nc* command. The concatenated signals are obtained by "gluing" together the payloads of the constituent signals, and they come in fixed sizes. In *SONET*, these are called STS-*N*c Synchronous Payload Envelopes (SPEs), where *N* = 3*X* and *X* is restricted to the values 1, 4, 16, 64, or 256..

mode *sts-nc*

Syntax Description

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Controller configuration

Command History

Release	Modification
XE 3.18 SP	Support for this command was introduced on NCS 4200 Series.

Usage Guidelines

The command is used to concatenate continuous STS into a bundle. supported modes are STS-3c, STS-12c, STS-48c, STS-192c.

Examples

The following example shows the configuration of STS-Nc - contiguous concatenation:

```
enable
configure terminal
controller MediaType 0/5/0
mode sonet
controller sonet 0/5/0
rate oc12
sts-1 1-3 mode sts-3c
end
```

Related Commands

Command	Description
controller sonet	Configures the SONET mode.
show controller sonet	Displays SONET controller configuration.

mode t3/e3

To set the T3/E3 controller in T3/E3 mode and create a logical T3/E3 controller, use the mode command in controller configuration mode.

mode t3.e3

Syntax Description

t3/e3	To set the T3/E3controller into T3/E3 mode and create a logical T3/E3 controller, use the mode command in controller configuration mode.

Command Default

The controller mode is disabled.

Command Modes

Controller configuration

Command History

Command History

Release	Modification
XE 3.18SP	This command was introduced.

Usage Guidelines

Use this command to enable the port in T3 mode. When the port is enabled for T3, it can be used for clear channel mode or channelized T3 mode based on configuration.

Examples

The following example shows how to create the local loopback on the controller :

```
Router(config-controller)# mode t3/e3
```

Related Commands

Command	Description
controller media-type	Enters controller configuration mode.

mode two-way

To enable two-way operational mode for the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT), use the **modetwo-way**command in satellite initial configuration mode. To revert to one-way operational mode, use the **no** form of this command.

mode two-way
no mode two-way

Syntax Description

This command has no arguments or keywords.

Command Default

Two-way mode is enabled.

Command Modes

Satellite initial configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

This command is typically used by an installation technician. Do not use this command unless your satellite service provider instructs you to perform the satellite initial configuration and provides all necessary parameter values.

Examples

The following example shows how to specify two-way operational mode:

```
Router(sat-init-config)# mode two-way
```

The following example shows how to specify one-way operational mode:

```
Router(sat-init-config)# no mode two-way
```

mode vc-1x

Use this command to configure mode VC-1x mode.

mode vc-1x

Syntax Description

Syntax Description

None

Command Default

None

Command Modes

Controller configuration

Command History

Release	Modification
XE Everest 16.6.1	This command was integrated into the Cisco NCS 4200 Series and Cisco ASR 900 Series.

Usage Guidelines

When you configure mode VC-1x, seven TUG-2 payloads are created. TUG-2 payloads can be of two types, VC-11 and VC-12. Default for TUG-2 payload mode is VC-11. TUG-2 payload VC-11 can be configured as VC or T1 and the range is 1 to 4. TUG-2 payload VC-12 can be configured as VC or E1 and the range is 1 to 3.

Examples

```
enable
configure terminal
controller sdh 0/5/0
rate stm1
no ais-shut
alarm-report all
clock source internal
overhead s1s0 0
aug mapping au-4
au-4 1
clock source internal
mode tug-3
tug-3 1
mode VC1x
tug-2 1 payload VC11
tug-2 2 payload VC11
tug-2 3 payload VC11
tug-2 4 payload VC11
tug-2 5 payload VC11
tug-2 6 payload VC11
tug-2 7 payload VC11
end
```

Related Commands

Command	Description
show running configuration	Verifies mode vc-1z configuration.

mode vc-4

Use this command to configure mode VC4 CEP.

mode vc-4

Syntax Description

Syntax Description

None

Command Default

None

Command Modes

Controller configuration

Command History

Release	Modification
XE Everest 16.6.1	This command was integrated into the Cisco NCS 4200 Series and Cisco ASR 900 Series.

Usage Guidelines

CEP mode is used to encapsulate SDH payload envelopes (SPEs) like VC11, VC12, VC4, or VC4-Nc over PSN. In this mode, the bytes from the corresponding SPE are sent out as they arrive on the TDM line. The interface is considered as a continuous framed bit stream. The packetization of the stream is done according to IETF RFC 4842. The supported ports are STM1, STM4, STM16, and STM64.

Examples

```
enable
configure terminal
controller sdh 0/5/0
rate stm 4
aug mapping au-4
au-4 1
mode vc4
cem-group 100 cep
end
```

Related Commands

Command	Description
show running configuration	Verifies mode VC-4 configuration.

mode vc4-Nc

Use this command to configure mode VC-4 Nc under AU-4.

mode vc4-Nc

Syntax Description

Syntax Description

None

Command Default

None

Command Modes

Controller configuration

Command History

Release	Modification
XE Everest 16.6.1	This command was integrated into the Cisco NCS 4200 Series and Cisco ASR 900 Series.

Usage Guidelines

CEP mode is used to encapsulate SDH payload envelopes (SPEs) like VC11, VC12, VC4, or VC4-Nc over PSN. In this mode, the bytes from the corresponding SPE are sent out as they arrive on the TDM line. The interface is considered as a continuous framed bit stream. The packetization of the stream is done according to IETF RFC 4842. The supported ports are STM1, STM4, STM16, and STM64.

Examples

```
enable
configure terminal
controller sdh 0/5/0
au-4 1-4 mode vc4-4c
cem-group 100 cep
end
```

Related Commands

Command	Description
show running configuration	Verifies configuration.

mode vt-15

To configure the path operation mode, use the **mode vt-15** command in controller configuration STS mode.

mode vt-15

Syntax Description

vt-15	Specifies the mode of operation.

Command Default

None

Command Modes

Controller configuration STS

Command History

Release	Modification
15.1(01)S	This command was introduced on the Cisco 7600 routers.

Examples

This example shows how to configure the **mode vt-15**:

```
Router(config)# controller sonet-acr 1
Router(config-controller)#
sts-1 2
Router(config-ctrlr-sts1)# mode vt-15
```

Related Commands

Command	Description
sts-1	Configures the Synchronous Transport Signal (STS) (level)-1 in the SONET hierarchy.
vtg	Configures the (CESoPSN) CEM group.
controller sonet-acr	Configures the SONET Access Circuit Redundancy (ACR) virtual controller.

mode t3

Use this command to configure T3 mode.

mode t3

Syntax Description

Syntax Description

None

Command Default

None

Command Modes

Controller configuration

Command History

Release	Modification
XE Everest 16.6.1	This command was integrated into the Cisco NCS 4200 Series and Cisco ASR 900 Series.

Usage Guidelines

You can change the mode of a controller only when there are no subinterfaces defined for the controller.

Examples

```
enable
configure terminal
controller sdh 0/5/0
rate stm4
au-4 1
mode tug-3
tug-3 1
mode t3
cem-group 100 unframed
end
```

Related Commands

Command	Description
show running configuration	Verifies configuration.

mode tug-3

Use this command to configure mode Tributary Unit group type 3 (TUG-3) number that has been mapped to an AU-4.

mode tug-3

Syntax Description

Syntax Description

None

Command Default

None

Command Modes

Controller configuration

Command History

Release	Modification
XE Everest 16.6.1	This command was integrated into the Cisco NCS 4200 Series and Cisco ASR 900 Series.

Usage Guidelines

An AUG of an STM-1 can be derived from either AU-3s or an AU-4. Use the **aug mapping au-4** configuration controller command to map the AUG to a TUG-3. Configuring the **au-4** command enables you to enter configuration controller tug3 command mode and creates a serial interface.

Mode TUG-3 creates three TUG-3 paths. TUG-3 range is 1 to 3.

Examples

```
enable
configure terminal
controller sdh 0/5/0
rate stm4
au-4 1
mode tug-3
end
```

Related Commands

Command	Description
show running configuration	Verifies TUG-3 configuration.

modem dtr-delay

To control the time that a data terminal ready (DTR) signal is held down when a line clears, use the **modemdtr-delay** command in line configuration mode. To restore the default hold down time, use the **no** form of this command.

modem dtr-delay *seconds*
no modem dtr-delay *seconds*

Syntax Description

seconds	Number of seconds. The default is 5.

Command Default

The default DTR signal hold down time is 5 seconds.

Command Modes

Line configuration

Command History

Release	Modification
12.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to reduce the time that a DTR signal is held down after an asynchronous line clears and before the DTR signal is raised again to accept new calls. Incoming calls may be rejected in heavily loaded systems even when modems are unused because the default DTR hold down interval may be too long. The**modemdtr-delay** command is designed for lines used for an unframed asynchronous session such as Telnet. Lines used for a framed asynchronous session such as PPP should use the **pulse-time** interface command.

Examples

The following example shows how to specify a DTR hold down interval of 2 seconds:

```
Router(config)# line 7
Router(config-line)# modem dtr-delay 2
```

Related Commands

Command	Description
pulse-time	Enables pulsing DTR signal intervals on serial interfaces.

monitoring

To enable monitoring of all optical transceivers and to specify the time period for monitoring the transceivers, use the **monitoring**command in transceiver type configuration mode. To disable the monitoring, use the **no** form of this command.

monitoring [**interval** *seconds*]
no monitoring [**interval**]

Syntax Description

interval *seconds*	(Optional) Specifies the time interval for monitoring optical transceivers; valid range is 300 to 3600, in seconds, and the default interval time is 600.

Command Default

The interval time is 600 seconds.

Command Modes

Transceiver type configuration (config-xcvr-type)

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.2(33)SXH	This command was modified. The**interval** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.2(2)SNI	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

You need digital optical monitoring (DOM) feature and transceiver module compatibility information to configure the **monitoring** command. Refer to the compatibility matrix to get the lists of Cisco platforms and minimum required software versions to support Gigabit Ethernet transceiver modules.

Gigabit Ethernet Transceivers transmit and receive Ethernet frames at a rate of a gigabit per second, as defined by the IEEE 802.3-2008 standard. Cisco's Gigabit Ethernet Transceiver modules support Ethernet applications across all Cisco switching and routing platforms. These pluggable transceivers offer a convenient and cost effective solution for the adoption in data center, campus, metropolitan area access and ring networks, and storage area networks.

The **monitoring** command helps you to enable DOM feature and to evaluate threshold violations for all transceiver types. The **interval**keyword enables you to change the default polling interval.For example, if you set the interval as 1500 seconds, this setting causes a delay (of 1500 seconds) for the trap to be sent out by the Simple Network Management Protocol (SNMP) manager running on Cisco IOS software.

Examples

This example shows how to enable monitoring of optical transceivers and set the interval time for monitoring to 1500 seconds:

```
Router# configure terminal
Router(config)# transceiver type all
Router(config-xcvr-type)# monitoring interval 1500
```

This example shows how to disable monitoring for all transceiver types:

```
Router(config-xcvr-type)# no monitoring
```

Related Commands

Command	Description
transceiver type all	Enables monitoring on all transceivers.

mop enabled

To enable an interface to support the Maintenance Operation Protocol (MOP), use the **mopenabled** command in interface configuration mode. To disable MOP on an interface, use the **no** form of this command.

mop enabled
no mop enabled

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled on Ethernet interfaces and disabled on all other interfaces.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example enables MOP for serial interface 0:

```
Router(config)# interface serial 0
Router(config-if)# mop enabled
```

Related Commands

Command	Description
mop retransmit-timer	Configures the length of time that the Cisco IOS software waits before sending boot requests again to a MOP server.
mop retries	Configures the number of times the Cisco IOS software will send boot requests again to a MOP server.
mop sysid	Enables an interface to send out periodic MOP system identification messages.

mop sysid

To enable an interface to send out periodic Maintenance Operation Protocol (MOP) system identification messages, use the **mopsysid** command in interface configuration mode. To disable MOP message support on an interface, use the **no** form of this command.

mop sysid
no mop sysid

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can still run MOP without having the background system ID messages sent. This command lets you use the MOP remote console, but does not generate messages used by the configurator.

Examples

The following example enables serial interface 0 to send MOP system identification messages:

```
Router(config)# interface serial 0
Router(config-if)# mop sysid
```

Related Commands

Command	Description
mop device-code	Identifies the type of device sending MOP sysid messages and request program messages.
mop enabled	Enables an interface to support the MOP.

mtu

To adjust the maximum packet size or maximum transmission unit (MTU) size, use the **mtu** command in interface configuration mode, connect configuration mode, or xconnect subinterface configuration mode. To restore the MTU value to its original default value, use the **no** form of this command.

mtu *bytes* **mtu command**
no mtu

Syntax Description

bytes	MTU size, in bytes.

Command Default

The table below lists default MTU values according to media type.

Table 24: Default Media MTU Values

Media Type	Default MTU (Bytes)
Ethernet	1500
Serial	1500
Token Ring	4464
ATM	4470
FDDI	4470
HSSI (HSA)	4470

Command Modes

Interface configuration (config-if) Connect configuration (xconnect-conn-config) xconnect subinterface configuration (config-if-xconn)

Command History

Release	Modification
10.0	This command was introduced.
12.0(26)S	This command was modified. This command was updated to support the connect configuration mode for Frame Relay Layer 2 interworking.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX. Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	This command was modified. Support for this command was introduced on the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.

Release	Modification
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4. This command supports the xconnect subinterface configuration mode.

Usage Guidelines

Each interface has a default maximum packet size or MTU size. This number generally defaults to the largest size possible for that interface type. On serial interfaces, the MTU size varies but cannot be set to a value less than 64 bytes.

Note The connect configuration mode is used only for Frame Relay Layer 2 interworking.

Changing the MTU Size

Changing the MTU size is not supported on a loopback interface.

Changing the MTU size on a Cisco 7500 series router results in the recarving of buffers and resetting of all interfaces. The following message is displayed: RSP-3-Restart:cbus complex .

You can configure native Gigabit Ethernet ports on the Cisco 7200 series router to a maximum MTU size of 9216 bytes. The MTU values range from 1500 to 9216 bytes. The MTU values can be configured to any range that is supported by the corresponding main interface.

Protocol-Specific Versions of the mtu Command

Changing the MTU value with the **mtu** interface configuration command can affect values for the protocol-specific versions of the command (the **ipmtu** command, for example). If the value specified with the **ipmtu** interface configuration command is the same as the value specified with the **mtu** interface configuration command, and you change the value for the **mtu** interface configuration command, the **ipmtu** value automatically matches the new **mtu** interface configuration command value. However, changing the values for the **ipmtu** configuration commands has no effect on the value for the **mtu** interface configuration command.

ATM and LANE Interfaces

ATM interfaces are not bound by what is configured on the major interface. By default, the MTU on a subinterface is equal to the default MTU (4490 bytes). A client is configured with the range supported by the corresponding main interface. The MTU can be changed on subinterfaces, but it may result in recarving of buffers to accommodate the new maximum MTU on the interface.

VRF-Aware Service Infrastructure Interfaces

The mtu command does not support the VRF-Aware Service Infrastructure (VASI) type interface.

Cisco 7600 Valid MTU Values

On the Cisco 7600 platform, the following valid values are applicable:

- For the SVI ports: from 64 to 9216 bytes
- For the GE-WAN+ ports: from 1500 to 9170 bytes
- For all other ports: from 1500 to 9216 bytes

You can receive jumbo frames on access subinterfaces also. The MTU values can be configured to any range that is supported by the corresponding main interface. If you enable the jumbo frames, the default is 64 bytes for the SVI ports and 9216 bytes for all other ports. The jumbo frames are disabled by default.

Cisco uBR10012 Universal Broadband Router

While configuring the interface MTU size on a Gigabit Ethernet SPA on a Cisco uBR10012 router, consider the following guidelines:

- The default interface MTU size accommodates a 1500-byte packet, plus 22 additional bytes to cover the following overhead:
  - Layer 2 header--14 bytes
  - Dot1Q header--4 bytes
  - CRC--4 bytes
- If you are using MPLS, be sure that the **mplsmtu** command is configured with a value less than or equal to the interface MTU.
- If you are using MPLS labels, you should increase the default interface MTU size to accommodate the number of MPLS labels. Each MPLS label adds 4 bytes of overhead to a packet.

Note For the Gigabit Ethernet SPAs on the Cisco uBR10012 router, the default MTU size is 1500 bytes. When the interface is being used as a Layer 2 port, the maximum configurable MTU is 9000 bytes.

Examples

The following example shows how to specify an MTU of 1000 bytes:

```
Router(config)# interface serial 1
Router(config-if)# mtu 1000
```

Cisco uBR10012 Universal Broadband Router

The following example shows how to specify an MTU size on a Gigabit Ethernet SPA on the Cisco uBR10012 router:

```
Router(config)# interface GigabitEthernet3/0/0
Router(config-if)# mtu 1800
```

Related Commands

Command	Description
encapsulation smds	Enables SMDS service on the desired interface.
ip mtu	Sets the MTU size of IP packets sent on an interface.

national bit (controller)

To set the E3 national bit in the G.751 frame used by the E3 controller, use the national bit command in controller configuration mode. To return to the default E3 controller national bit, use the no form of this command.

national bit {**0** | **1**}
no national bit

Syntax Description

0	Sets the E3 national bit in the G.751 frame to 0.
1	Sets the E3 national bit in the G.751 frame to 1. This is the default.

Command Default

The default value is 1.

Command Modes

Controller configuration

Command History

Release	Modification
11.1 CA	This command was introduced.
12.2(11)YT	This command was integrated into Cisco IOS Release 12.2(11)YT and implemented on the following platforms: Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3660 series, Cisco 3725, and Cisco 3745 routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines

When G.751 framing is used, bit 11 of the G.751 frame is reserved for national use and is set to 1 by default.

Configure national bit 1 only when required for interoperability with your telephone company.

To verify the national bit configured on the interface, use the **showcontrollersserial** EXEC command.

Examples

The following example sets the national bit to 1 on an E3 controller in slot 1, port 0:

```
Router(config)# controller e3 1/0
Router(config-controller)# national bit 1
```

Related Commands

show controllers serial	Displays information that is specific to the interface hardware.

national bit (interface)

To set the E3 national bit in the G.751 frame used by the PA-E3 port adapter, use the **nationalbit**command in interface configuration mode. To return to the default E3 interface national bit, use the **no** form of this command.

national bit {**0** | **1**}
no national bit

Syntax Description

0	Sets the E3 national bit in the G.751 frame to 0. This is the default.
1	Sets the E3 national bit in the G.751 frame to 1.

Command Default

The default value is 0.

Command Modes

Interface configuration

Command History

Release	Modification
11.1 CA	This command was introduced.

Usage Guidelines

The **nationalbit** command sets bit 12 in the E3 frame.

To verify the national bit configured on the interface, use the **showcontrollersserial** EXEC command.

Examples

The following example sets the national bit to 1 on the PA-E3 port adapter in slot 1, port adapter slot 0, interface 0:

```
Router(config)# interface serial 1/0/0
Router(config-if)# national bit 1
```

Related Commands

Command	Description
international bit	Sets the E3 international bit in the G.751 frame used by the PA-E3 port adapter.
show controllers serial	Displays information that is specific to the interface hardware.

national reserve

To set the E1 national bit, use the**nationalreserve**command in interface configuration mode. To return to the default E1 national bit, use the**no** form of this command.

national reserve {**0** | **1**} {**0** | **1**} {**0** | **1**} {**0** | **1**} {**0** | **1**} {**0** | **1**}
no national reserve

Syntax Description

0	Sets any of the six required E1 national bits in the G.751 frame to 0.
1	Sets any of the six required E1 national bits in the G.751 frame to 1. This is the default.

Command Default

111111

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)XE	This command was introduced.
12.0(7)XE1	This command was implemented on the Cisco 7100 series routers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command applies only for E1. This command not only sets the national reserve bits but also sets the international bit as well. The far left digit represents the international bit. All six digits must be present for the pattern to be valid.

Examples

On Cisco 7100 series routers, the following example sets the E1 national bit on interface 1 on the port adapter in slot 0 to no scrambling:

```
Router(config)# interface atm 1/0
Router(config-if)# national reserve 011011
```

negotiation

To enable advertisement of speed, duplex mode, and flow control on a Gigabit Ethernet interface, use the**negotiation**command in interface configuration mode. To disable automatic negotiation, use the **nonegotiationauto** command.

negotiation {**forced** | **auto**}
no negotiation auto

Syntax Description

forced	Disables flow control and configures the Gigabit Ethernet interface in 1000/full-duplex mode. This keyword is not supported on the 2-port 10/100/1000 Gigabit Ethernet shared port adapter (SPA) on the Cisco 7304 router.
auto	Enables the autonegotiation protocol to configure the speed, duplex, and automatic flow control of the Gigabit Ethernet interface. This is the default.

Command Default

Autonegotiation is enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.1CC	This command was introduced.
12.0(7)S	This command was modified. The forced keyword was added.
12.0(6)T	This command was modified. The forced keyword was added.
12.1(3a)E	This command was integrated into Cisco IOS Release 12.1E and implemented on the Cisco 7200-I/O-GE+E controller.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(20)S2	This command was implemented on the 2-port 10/100/1000 Gigabit Ethernet SPA on the Cisco 7304 router. The **forced** keyword is not supported.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.

Usage Guidelines

The **negotiation**command is applicable to the Gigabit Ethernet interface of the Cisco 7200-I/O-GE+E and interfaces on the 2-port 10/100/1000 Gigabit Ethernet SPA that are using fiber media. The **negotiationauto**command is used instead of the **duplex** and **speed** commands (which are used on Ethernet and Fast Ethernet interfaces, and interfaces on the 2-port 10/100/1000 Gigabit Ethernet SPA that are using RJ-45 media) to automatically configure the duplex and speed settings of the interfaces.

The **negotiationforced** command is used to configure the Gigabit Ethernet interface of the Cisco 7200-I/O-GE+E to be 1000/full-duplex only and to disable flow control. The **negotiationforced** command is not supported by the 2-port 10/100/1000 Gigabit Ethernet SPA.

The Gigabit Ethernet interface of the Cisco 7200-I/O-GE+E and the interfaces on the 2-port 10/100/1000 Gigabit Ethernet SPA that are using fiber media are restricted to 1000 Mbps/full-duplex only. Autonegotiation advertises and negotiates only to these values.

The **nonegotiationauto** command is used to disable the autonegotiation in the Cisco 3800 series routers. If the speed is set to 1000 Mbps and full-duplex is set for the Gigabit Ethernet interface in small form-factor pluggable (SFP) mode, then the autonegotiation is disabled (forced mode) using the **nonegotiationauto** command.

However, for RJ-45 media the autonegotiation is always enabled for fixed speed and duplex setting. For SFP mode of operation, the autonegotiation can be disabled by using the **nonegotiationauto** command.

Cisco uBR10012 Universal Broadband Router

Autonegotiation is enabled by default and can be disabled on the 5-port Gigabit Ethernet SPA. During autonegotiation, advertisement for flow control, speed, and duplex occurs. If autonegotiation is disabled on one end of a link, it must be disabled on the other end of the link. If one end of a link has autonegotiation disabled and the other end of the link does not, the link does not come up properly on both ends. Flow control is always negotiated when autonegotiation is enabled.

Note Autonegotiation is not supported on the 1-port 10-Gigabit Ethernet SPA in Cisco IOS Release 12.2(33)SCB.

Examples

The following example shows how to enable the second interface (port 1) on a 2-port 10/100/1000 Gigabit Ethernet SPA for autonegotiation, where the SPA is installed in the bottom subslot (1) of the modular services card (MSC), and the MSC is installed in slot 2 of the Cisco 7304 router:

```
Router(config)# interface gigabitethernet 2/1/1
Router(config-if)# media-type gbic
Router(config-if)# negotiation auto
```

The following example shows how to disable the second interface (port 1) on a 2-port 10/100/1000 Gigabit Ethernet SPA for autonegotiation, where the SPA is installed in the bottom subslot (1) of the MSC, and the MSC is installed in slot 2 of the Cisco 7304 router:

```
Router(config)# interface gigabitethernet 2/1/1
Router(config-if)# no negotiation auto
```

Related Commands

Command	Description
show interfaces gigabitethernet	Displays information about the Gigabit Ethernet interfaces.

neighbor (VPLS)

To specify the type of tunnel signaling and encapsulation mechanism for each Virtual Private LAN Service (VPLS) peer, use the **neighbor** command in L2 VFI manual configuration mode. To disable a split horizon, use the **no** form of this command.

neighbor *remote-router-id* *vc-id* {**encapsulation** *encapsulation-type* | **pw-class** *pw-name*} [**no-split-horizon**]
no **neighbor** *remote-router-id* [*vc-id*]

Syntax Description

remote-router-id	Remote peer router identifier. The remote router ID can be any IP address, as long as it is reachable.
vc-id	32-bit identifier of the virtual circuit between the routers.
encapsulation	Specifies tunnel encapsulation.
encapsulation-type	Specifies the tunnel encapsulation type; valid values are **l2tpv3** and **mpls**.
pw-class	Specifies the pseudowire class configuration from which the data encapsulation type is taken.
pw-name	Name of the pseudowire class.
no-split-horizon	(Optional) Disables the Layer 2 split horizon forwarding in the data path.

Command Default

Split horizon is enabled.

Command Modes

L2 VFI manual configuration (config-vfi)

Command History

Release	Modification
12.2(18)SXF	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was modified. This command was updated so that the remote router ID need not be the LDP router ID of the peer.
Cisco IOS XE Release XE 3.7S	This command was integrated into Cisco IOS XE Release XE 3.7S.

Usage Guidelines

In a full-mesh VPLS network, keep split horizon enabled to avoid looping.

With the introduction of VPLS Autodiscovery, the remote router ID no longer needs to be the LDP router ID. The address that you specify can be any IP address on the peer, as long as it is reachable. When VPLS Autodiscovery discovers peer routers for the VPLS, the peer router addresses might be any routable address.

Examples

This example shows how to specify the tunnel encapsulation type:

```
Device(config-vfi)# l2 vfi vfi-1 manual
Device(config-vfi)# vpn 1
Device(config-vfi)# neighbor 172.16.10.2 4 encapsulation mpls
```

This example shows how to disable the Layer 2 split horizon in the data path:

```
Device(config-vfi)# l2 vfi vfi-1 manual
Device(config-vfi)# vpn 1
Device(config-vfi)# neighbor 172.16.10.2 4 encapsulation mpls no-split-horizon
```

Related Commands

Command	Description
l2 vfi manual	Creates a Layer 2 VFI.

network-clock (BITS)

To configure BITS port signaling types, use the **network-clock**command in global configuration mode. To disable the BITS port signaling types, use the **no** form of this command.

network-clock slot *slot* **bits** *number* {**2m** | **e1** [**crc4**] | **j1** [**esf**] | **t1** [{**d4** | **esf** [{**133ft** | **266ft** | **399ft** | **533ft** | **655ft**}]}]}
no network-clock slot *slot* **bits** *number* {**2m** | **e1** [**crc4**] | **j1** [**esf**] | **t1** [{**d4** | **esf** [{**133ft** | **266ft** | **399ft** | **533ft** | **655ft**}]}]}

Syntax Description

slot	Selects the slot.
slot	Specifies backplane slot number.
bits	Specifies BITS port signaling types.
number	Specifies the BITS port number starting from 0.
2m	Specifies 2.048 MHz square wave signal type.
e1	Specifies E1 signal type.
j1	Specifies Japan J1 signal type.
t1	Specifies T1 signal type.
crc4	E1 CRC4 framing mode.
esf	T1 ESF framing mode.
d4	T1 D4 framing mode.
133ft	Line Build-Out Select 0 to 133 feet.
266ft	Line Build-Out Select 0 to 266 feet.
399ft	Line Build-Out Select 0 to 399 feet.
533ft	Line Build-Out Select 0 to 533 feet.
655ft	Line Build-Out Select 0 to 655 feet.

Command Default

T1, ESF, 133ft

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRD1	This command was introduced on the Cisco series 7600 router for the 76-ES+XT-2TG3CXL and 76-ES+XT-4TG3CXL.

Usage Guidelines

For 76-ES+XT-2TG3CXL and 76-ES+XT-4TG3CXL line cards, the BITS port number is always 0 because there is only one BITS port.

Examples

The following example shows how to configure the BITS port and 10GE interface as clock sources:

```
Router(config)# network-clock select 2 slot 1 ?
  bits    Network clock source is bits interface
  global  Configure the source as global
  local   Configure the source as local
  <cr>

Router(config)# network-clock select 2 slot 1 bits 0 ?
  global  Configure the source as global
  local   Configure the source as local
  <cr>

Router(config)# network-clock select 3 ?
  controller  Select the controller that should source the clock
  interface   Select the interface that should source the clock
  slot        Select the slot that should source the clock
  system      Select the system clock as source

Router(config)# network-clock select 3 interface TenGigabitEthernet 1/1
```

The following example shows how to configure the BITS port signal type and framing mode:

```
Router(config)# network-clock slot 1 bits 0 ?
  2m  2.048MHz square wave signal type
  e1  E1 signal type
  j1  Japan J1 signal type
  t1  T1 signal type

Router(config)# network-clock slot 1 bits 0 t1 ?
  d4   T1 D4 framing mode
  esf  T1 ESF framing mode

Router(config)# network-clock slot 1 bits 0 t1 d4 ?
  133ft  Line Build-Out Select 0 to 133 feet
  266ft  Line Build-Out Select 133 to 266 feet
  399ft  Line Build-Out Select 266 to 399 feet
  533ft  Line Build-Out Select 399 to 533 feet
  655ft  Line Build-Out Select 533 to 655 feet

Router(config)# network-clock slot 1 bits 0 j1 ?
  esf  J1 ESF framing mode

Router(config)# network-clock slot 1 bits 0 e1 ?
  crc4  E1 CRC4 framing mode

Router(config)# network-clock slot 1 bits 0 2m ?
  <cr>
```

Related Commands

Command	Description
show network-clocks	Displays the current configured and active network clock sources.

Command	Description
show platform hardware network-clocks	Displays network clocks for an ES+ line card.

network-clock clear lockout

To clear the lock-out on a clock source, use the network-clock clear lockout command in the privileged EXEC mode.

Cisco 7600 Series Routers
network-clock clear lockout interface *slot/card/port* | **external** *slot/card/port* **2048K** | **e1** {**cas** | **crc4** | **fas**}

Cisco ASR 1000 Series Routers
network-clock clear lockout external {*slot/card/port* | **R0** | **R1**} **T1** {**d4** | **esf** | **sf**}

Syntax Description

external	Specifies external interface (BITS/SSU/GPS).
slot/card/port	Slot number/Card number/Port number.
R0	Specifies the network synchronization mcprp RP0 bits for source slot.
R1	Specifies the network synchronization mcprp RP1 bits for source slot.
T1	Specifies the T1 signal mode input.
d4	Specifies the D4 super frame signal mode.
esf	Specifies the extended super frame signal mode.
sf	Specifies the super frame signal mode.
2048k	Specifies the option 1 2048KHz on the BITS/SSU port.
e1	Specifies the E1 signal mode.
cas	Specifies the E1 Channel Associated Signal (CAS) mode.
crc4	Specifies the E1 with crc4 signal mode.
fas	Specifies the E1 Frame Alignment Signal mode.

Command Default

No default values are available.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.2.0S	This command was integrated into Cisco ASR 1000 Series routers.
Cisco IOS Release 12.2(33)SRE	This command was introduced on the Cisco 7600 Series routers.

Examples

The following example shows how to clear the lock out on a clock source:

```
C7600(config)# network-clock clear lockout external 0/0/0 e1 2048k
ASR1000(config)# network-clock clear lockout external 0/0/0 t1 esf
```

network-clock hold-off global

To configure the hold-off time, use the network-clock hold-off global command in the global configuration mode.

network-clock hold-off *timer* **global**

Syntax Description

timer	Hold-off time, in milliseconds. The range is from 50 to 10000. The default is 300. If you do not want the hold off time, set the timer value to 0.
global	Configures the hold-off timer globally.

Command Default

The default value is 300 milliseconds on Cisco ASR 901 Series Aggregation Services Routers.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2.0S	This command was integrated into Cisco ASR 1000 Series routers.
Cisco IOS Release 12.2(33)SRE	This command was introduced on the Cisco 7600 Series routers.
15.1(2)SNG	This command was implemented on Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

The hold-off timer can also be configured in the interface configuration mode. It displays a warning message for values below 300 milliseconds and above 1800 milliseconds.

Examples

The following example shows how to configure the hold-off timer in the global configuration mode:

```
Router(config)# network-clock hold-off 50 global
```

network-clock input-source

To assign a controller to be the primary or secondary clock source use the **network-clock input-source***priority* command. To set the controller to be a primary clock source, set the value of priority for the input source to be low value, such as 2, (a low value indicates a high priority). To remove the clock source, use the **no** form of this command

network-clock input-source *priority* **controller t1/e1***slot/bay/port*

no network-clock input-source *priority* **controller t1/e1** *slot/bay/port*

Syntax Description

network-clock input-source *priority*	The network-clock input-source priority command selects the configured controller clock as the backplane clock source.
controller t1/e1	Sets the controller into T1 or E1 signal mode.
priority	Sets the controller to be a primary clock source.
slot/bay/port	Specifies slot, bay and port number

Command Modes

Global configuration

Command History

Release	Modification
XE 3.18SP	Support for this command was introduced on NCS 4200 Series.
XE Everest 16.5.1	This command was introduced on the Cisco ASR 900 Series Routers and Cisco NCS 4200 Series.

Usage Guidelines

This command is used to assign controller to be the primary or secondary clock source.

Examples

```
enable
configure terminal
network-clock input-source 1controller E1/T10/5/0
```

network-clock set lockout

To lock out a clock source, use the network-clock set lockout command in the privileged EXEC mode. On the Cisco ASR 901 Series Aggregation Services Routers, use the **network-clock clear lockout** command to remove the lockout in global configuration mode.

Cisco 7600 Series Routers

{**network-clock set lockout internal** *slot/card/port* | **external** *slot/card/port* **2048K** | **e1** {**cas** | **crc4** | **fas**}}

Cisco ASR 1000 Series Routers

network-clock set lockout external {*slot/card/port* | **R0** | **R1**} **T1** {**d4** | **esf** | **sf**}

Cisco ASR 901 Cisco ASR 901 Series Aggregation Services Routers

network-clock set lockout {**interface** *interface-name slot/port* | **external** *slot/card/port*}

network-clock clear lockout

Syntax Description

external	Specifies external interface (BITS/SSU/GPS).
slot/card/port	Slot number/card number/port number.
R0	Specifies the network synchronization mcprp RP0 bits for the source slot.
R1	Specifies the network synchronization mcprp RP1 bits for the source slot.
T1	Specifies the T1 signal mode input.
d4	Specifies the D4 super frame signal mode.
esf	Specifies the extended super frame signal mode.
sf	Specifies the super frame signal mode.
2048k	Specifies the option 1 2048KHz on the BITS/SSU port.
e1	Specifies the E1 signal mode.
cas	Specifies the E1 Channel Associated Signal (CAS) mode.
crc4	Specifies the E1 with crc4 signal mode.
fas	Specifies the E1 Frame Alignment Signal mode.
interface	Specifies the interface.
interface-name	Specifies the interface name.

Command Default

No default values are available.

Command Modes

- Global configuration (config)
- Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.2.0S	This command was integrated into Cisco ASR 1000 Series routers.
Cisco IOS Release 12.2(33)SRE	This command was introduced on the Cisco 7600 Series routers.
15.1(2)SNG	This command was implemented on Cisco ASR 901 Series Aggregation Services Routers. The *interface-name* argument was added.

Usage Guidelines

The **network-clock set lockout** command locks out a clock source. A locked out clock source is not selected for SyncE.

To clear the lock-out on a source, use the **network-clock clear lockout** command.

Note Lock-out takes precedence over force switch, and force switch overrides the manual switch.

Examples

The following example shows how to lock out a clock source:

```
C7600(config)# network-clock set lockout external 2/0/0 e1 cas
ASR1000(config)# network-clock set lockout external R0 t1 esf
```

This example shows how to lockout the clock source on a Cisco ASR 901 Series Aggregation Services Router.

```
Router(config)# network-clock set lockout interface GigabitEthernet 0/1
```

network-clock synchronization ssm option

To configure the equipment to work in a synchronization network, use the **network-clock synchronization ssm option** command in the global configuration mode. To unconfigure the network-clock synchronization option, use the no form of this command.

network-clock synchronization ssm option option_id {**1** | **2** {**GEN1** | **GEN2**}}
no network-clock synchronization ssm option option_id {**1** | **2** {**GEN1** | **GEN2**}}

Syntax Description

option_id	The option_id can have the following values: • 1 - Refers to the synchronization networks design for Europe. This is the default value. (E1 framings are compatible with this option). • 2 - Refers to the synchronization networks design for the U.S. (T1 framings are compatible with this option).
GEN1	If option 2 is configured, then it specifies the generation ID as 1.
GEN2	If option 2 is configured, then it specifies the generation ID as 2.

Command Default

No default values are available.

Cisco ASR 901 Series Aggregation Services Routers

Option 1.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was integrated into Cisco ASR 1000 Series routers.
Cisco IOS Release 12.2(33)SRE	This command was introduced on the Cisco 7600 Series routers.
15.1(2)SNG	This command was implemented on Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Network-clock configurations that are not common between options need to be configured again.

On Cisco ASR 901 Series Aggregation Services Routers, the default value for the option_id keyword is 1. If you set the value to 2, you must specify the generation ID.

Examples

The following example shows how the **network-clocksynchronizationssmoption** command is used to configure the equipment to work in a synchronization network:

```
Router> enable
Router# configure terminal
Router(config)# network-clock synchronization automatic
Router(config)# network-clock synchronization ssm option 2 GEN1
```

Related Commands

Command	Description
network-clock eec	Configures the clocking system hardware with the desired parameters.

network-clock synchronization automatic

To enable the network clock synchronization selection process, use the network-clock synchronization automatic command in the global configuration mode. To disable the network clock synchronization selection process, use the no form of this command.

network-clock synchronization automatic
no network-clock synchronization automatic

Syntax Description

This command has no arguments or keywords.

Command Default

No default values are available.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2.0S	This command was integrated into Cisco ASR 1000 Series routers.
Cisco IOS Release 12.2(33)SRE	This command was introduced on the Cisco 7600 Series routers.

Usage Guidelines

This command disables the Cisco-specific network-clock process, and turns on G.781-based automatic clock synchronization selection process.

Examples

The following example shows how the network-clock synchronization automatic command is used to enable the network clock synchronization selection process:

```
Router(config)# network-clock synchronization automatic
```

network-clock synchronization mode QL-enabled

To configure the automatic selection process for the QL-enabled mode, use the network-clock synchronization mode QL-enabled command in the global configuration mode.

network-clock synchronization mode QL-enabled

Syntax Description

This command has no arguments or keywords.

Command Default

No default values are available.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2.0S	This command was integrated into Cisco ASR 1000 Series routers.
Cisco IOS Release 12.2(33)SRE	This command was introduced on the Cisco 7600 Series routers.
15.1(2)SNH	This command was introduced in Cisco ASR 901 Aggregation Services Routers.

Usage Guidelines

The automatic selection process for the QL-enabled mode is successful only if the Synchronous Ethernet interfaces are capable of sending Synchronization Status Messages (SSM).

Examples

The following example shows how to configure network clock synchronization (QL-enabled mode) in the global configuration mode:

```
Router(config)# network-clock synchronization mode QL-enabled
```

network-clock quality-level

To configure the Quality Level (QL) value for the Synchronization Status Messages (SSM) on a BITS port, use the network-clock quality-level command in the global configuration mode.

Cisco 7600 Series Routers
{**network-clock quality-level** {**rx** | **tx**} {**QL-PRC** | **QL-SSU-A** | **QL-SSU-B** | **QL-SEC** | **QL-DNU**} **external** *slot/card/port* **2048K** | **e1** {**cas** | **crc4** | **fas**}}

Cisco ASR 1000 Series Routers
network-clock quality-level {**rx** | **tx**} {**QL-PRS** | **QL-STU** | **QL-ST2** | **QL-TNC** | **QL-ST3** | **QL-ST3E** | **QL-SMC** | **QL-ST4** | **QL-DUS**} **external** {*slot/card/port* | **R0** | **R1**} **T1** {**d4** | **esf** | **sf**}

Syntax Description

rx	Specifies the received QL. The following values are available on Cisco ASR 1000 Series routers for the QL receive: • QL-PRS • QL-STU • QL-ST2 • QL-ST3 • QL-SMC • QL-ST4 • QL-DUS The following values are available on Cisco 7600 Series routers for the QL receive: • QL-PRC • QL-SSU-A • QL-SSU-B • QL-SEC • QL-DNU

tx	Specifies the trasmitted QL. The following values are available on Cisco ASR 1000 Series routers for the QL transmit: • QL-PRS • QL-STU • QL-ST2 • QL-ST3 • QL-SMC • QL-ST4 • QL-DUS The following values are available on Cisco 7600 Series routers for the QL transmit: • QL-PRC • QL-SSU-A • QL-SSU-B • QL-SEC • QL-DNU
external	Specifies the external interface (BITS/SSU/GPS).
slot /*card*/*port*	Slot number/Card number/Port number.
R0	Specifies the network synchronization RP0 bits for source slot.
R1	Specifies the network synchronization RP1 bits for source slot.
T1	Specifies the T1 signal mode output.
d4	Specifies the D4 super frame signal mode.
esf	Specifies the extended super frame signal mode.
sf	Specifies the super frame signal mode.
2048k	Specifies the option 1 2048KHz on the BITS/SSU port.
e1	Specifies the E1 signal mode.
cas	Specifies the E1 Channel Associated Signal (CAS) mode.
crc4	Specifies the E1 with crc4 signal mode.
fas	Specifies the E1 Frame Alignment Signal mode.

Command Default

No default values are available.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2.0S	This command was integrated into Cisco ASR 1000 Series routers.
Cisco IOS Release 12.2(33)SRE	This command was introduced on the Cisco 7600 Series routers.

Examples

The following example shows how to configure network-clock quality-level command in the global configuration mode:

```
C7600(config)# network-clock quality-level rx ql-prc external 0/0/0 e1 cas
ASR1000(config)# network-clock quality-level tx QL-ST2 external R0 t1 sf
```

no channelized

To configure the T3 controller for unchannelized mode, use the**nochannelized**configuration controller command. To configure channelized mode, use the **channelized**form of this command.

channelized
no channelized

Syntax Description

This command has no arguments or keywords.

Command Default

MTU size is set to 4470.

Command Modes

Configuration controller

Command History

Release	Modification
12.0(14)S	This command was introduced.
12.1(5a)E	This command was integrated into Cisco IOS Release 12.1(5a)E.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the no channelized configuration controller command to configure the T3 controller for unchannelized mode. When you configure the PA-MC-2T3+ on a Cisco 7500 series router with the no channelized command, the MTU size is set to 4470. In channelized mode, the default MTU size is 1500. The change in MTU sizes will cause a memory recarve and CBus complex to occur, disrupting all traffic on the router for several minutes.

The following message will be displayed when switching between channelized and unchannelized modes on a Cisco 7500 series router:

```
Change to subrate mode will cause cbus complex reset. Proceed? [yes/no]:
Y
```

Type Y for "yes" at the end of the warning. At the prompt, type ^Z to exit. You will exit configuration mode and enter unchannelized mode.

Examples

The following example configures unchannelized mode on a PA-MC-2T3+ in port adapter slot 1 of a VIP2 or VIP4 in a Cisco 7500 series router:

```
configure terminal
  controller T3 1/1/0
  no channelized
```

```
Change to subrate mode will cause cbus complex reset. Proceed? [yes/no]: Y
  ^Z
```

nrzi-encoding

To enable nonreturn-to-zero inverted (NRZI) line-coding format, use the **nrzi-encoding**command in interface configuration mode. To disable this capability, use the **no** form of this command.

nrzi-encoding [**mark**]
no nrzi-encoding

Syntax Description

mark	(Optional) Specifies that NRZI mark encoding is required on the PA-8T and PA-4T+ synchronous serial port adapters on Cisco 7200 and Cisco 7500 series routers . If the **mark** keyword is not specified, NRZI space encoding is used.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
11.3	The **mark** keyword was added for the Cisco 7200 series routers and Cisco 7500 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

All FSIP, PA-8T, and PA-4T+ interface types support nonreturn-to-zero (NRZ) and NRZI format. This is a line-coding format that is required for serial connections in some environments. NRZ encoding is most common. NRZI encoding is used primarily with EIA/TIA-232 connections in IBM environments.

Examples

The following example configures serial interface 1 for NRZI encoding:

```
Router(config)# interface serial 1
Router(config-if)# nrzi-encoding
```

The following example configures serial interface 3/1/0 for NRZI mark encoding:

```
Router(config)# interface serial 3/1/0
Router(config-if)# nrzi-encoding mark
```

O through R

outbound data-pid

Note Effective with Cisco IOS Release 12.4(2)T, this command is superseded by the **outboundpidmanagement** command. The **outbounddata-pid** command is still available, but use of the **outboundpidmanagement** command is recommended.

To specify the outbound data packet identification (PID) number, use the **outbounddata-pid** command in satellite initial configuration mode. To remove the PID number configuration, use the **no** form of this command.

outbound data-pid *number*
no outbound data-pid

Syntax Description

number	Packet identification (PID) number in the range from 1 to 8190.

Command Default

No default behavior or values

Command Modes

Satellite initial configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(2)T	This command was superseded by the**outboundpidmanagement** command.

Usage Guidelines

This command is typically used by an installation technician. Do not use this command unless your satellite service provider instructs you to perform the satellite initial configuration and provides all necessary parameter values.

Examples

The following example shows how to specify the outbound data PID number:

```
Router(sat-init-config)# outbound data-pid 3000
```

outbound data-rate

To specify the VSAT data rate, use the **outbounddata-rate** command in satellite initial configuration mode. To remove the data rate configuration, use the **no** form of this command.

outbound data-rate *rate*
no outbound data-rate

Syntax Description

rate	VSAT data rate in the range from 250000 to 73000000 bits per second.

Command Default

No default behavior or values

Command Modes

Satellite initial configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

This command is typically used by an installation technician. Do not use this command unless your satellite service provider instructs you to perform the satellite initial configuration and provides all necessary parameter values.

Examples

The following example shows how to specify the VSAT data rate:

```
Router(sat-init-config)# outbound data-rate 450000
```

outbound frequency

To specify the VSAT outbound frequency, use the **outboundfrequency** command in satellite initial configuration mode. To remove the outbound frequency configuration, use the **no** form of this command.

outbound frequency *frequency*
no outbound frequency

Syntax Description

frequency	VSAT outbound frequency in the range from 950000 to 2150000 kilohertz.

Command Default

No default behavior or values

Command Modes

Satellite initial configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

This command is typically used by an installation technician. Do not use this command unless your satellite service provider instructs you to perform the satellite initial configuration and provides all necessary parameter values.

Examples

The following example shows how to configure the VSAT outbound frequency:

```
Router(sat-init-config)# outbound frequency 950000
```

outbound id

To specify the VSAT outbound ID, use the **outboundid**command in satellite initial configuration mode. To remove the outbound ID configuration, use the **no** form of this command.

outbound id *number*
no outbound id

Syntax Description

number	ID number in the range from 0 to 255.

Command Default

No default behavior or values

Command Modes

Satellite initial configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

This command is typically used by an installation technician. Do not use this command unless your satellite service provider instructs you to perform the satellite initial configuration and provides all necessary parameter values.

Examples

The following example shows how to configure the VSAT outbound ID:

```
Router(sat-init-config)# outbound id 95
```

outbound modulation-type

To specify the VSAT modulation type, use the **outboundmodulation-type** command in satellite initial configuration mode. To remove the VSAT modulation type configuration, use the **no** form of this command.

outbound modulation-type {**DVB** | **TURBO_QPSK** | **8PSK**}
no outbound modulation-type

Syntax Description

DVB	Digital Video Broadcasting for satellite.
TURBO_QPSK	Turbo-coded quadrature Phase Shift Keying.
8PSK	Phase Shift Keying.

Command Default

No default behavior or values

Command Modes

Satellite initial configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

This command is typically used by an installation technician. Do not use this command unless your satellite service provider instructs you to perform the satellite initial configuration and provides all necessary parameter values.

Examples

The following example shows how to configure the VSAT modulation type:

```
Router(sat-init-config)# outbound modulation-type DVB
```

outbound sync ip address

To specify the outbound synchronization IP address, use the **outboundsyncipaddress** command in satellite initial configuration mode. To remove the outbound synchronization IP address configuration, use the **no** form of this command.

outbound sync ip address *address*
no outbound sync ip address

Syntax Description

address	Outbound synchronization IP address.

Command Default

No default behavior or values

Command Modes

Satellite initial configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

This command is typically used by an installation technician. Do not use this command unless your satellite service provider instructs you to perform the satellite initial configuration and provides all necessary parameter values.

Examples

The following example shows how to configure the outbound synchronization IP address:

```
Router(sat-init-config)# outbound sync ip address 10.2.2.2
```

outbound viterbi-rate

To specify the VSAT Viterbi code rate, use the **outboundviterbi-rate** command in satellite initial configuration mode. To return to the default rate, use the **no** form of this command.

outbound viterbi-rate *rate*
no outbound viterbi-rate

Syntax Description

rate	Viterbi code rate. It can be one of the following values: • **1/2** • **1/4** • **2/3** • **3/4** • **3/4(2.05)** • **3/4(2.1)** • **3/4(2.6)** • **5/6** • **6/7** • **7/8** • **8/9**

Command Default

No default behavior or values

Command Modes

Satellite initial configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

This command is typically used by an installation technician. Do not use this command unless your satellite service provider instructs you to perform the satellite initial configuration and provides all necessary parameter values.

Examples

The following example shows how to configure the VSAT Viterbi code rate:

```
Router(sat-init-config)# outbound viterbi-rate 3/4(2.6)
```

output

To enable out put of time of day messages using a 1PPS interface, use the **output** command in global configuration mode. To disable PTP output, use the **no** form of this command.

output 1pps *slot/bay* [**offset** *offset-value* [**negative**]] [**pulse-width** *pulse-amount* {**ns** | **us** | **ms**}]
no output 1pps *slot/bay* [**offset** *offset-value* [**negative**]] [**pulse-width** *pulse-amount* {**ns** | **us** | **ms**}]

Syntax Description

1pps	Configures the device to send 1 packet per second (1PPS) time of day messages using the RS422 port or 1PPS port. You can select 1PPS output with or without selecting a timing port.
slot	Slot of the 1PPS interface.
bay	Bay of the 1PPS interface.
offset	(Optional) Specifies an offset to compensate for a known phase error such as network asymmetry.
offset-value	Amount of offset in nanoseconds. The range is from 0 to 500,000,000.
negative	Specifies a negative offset 1PPS output value.
pulse-width	(Optional) Specifies a pulse width value.
pulse-amount	Amount of the pulse width. The range is from 1 to 4096. For 1PPS output using the RS422 port, you must specify a value of at least 2 ms.
ns	Specifies a pulse width value in nanoseconds.
us	Specifies a pulse width value in microseconds.
ms	Specifies a pulse width value in milliseconds.

Command Default

Time of day message output is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

If you want to provide output frequency clock, configure this command in PTP mode. This command only applies to platforms that have 1PPS ports.

Examples

The following example shows how to configure output clocking:

```
Device> enable
Device# configure terminal
Device(config)# ptp clock ordinary domain 0
Device(config-ptp-clk)# output 1pps 3/0 offset 10 pulse-width 1000 ms
Device(config-ptp-clk)# end
```

The following example shows the time of day (ToD) configuration on the 1588V2 subordinate and corresponding output:

```
Device> enable
Device# config terminal
Device(config)# ptp clock ordinary domain 0
Device(config-ptp-clk)# tod 3/3 cisco
Device(config-ptp-clk)# output 1pps 0 250 ns
Device(config-ptp-clk)# clock-port SLAVE slave
```

Related Commands

Command	Description
input	Enables PTP input clocking using the 1.544 Mhz, 2.048 Mhz, or 10 Mhz timing interface or phase using the 1PPS or RS-422 interface.

overhead c2

To set the SONET path overhead bytes in the frame header to a specific standards requirement or to ensure interoperability with equipment from another vendor, use the **overhead** command in SONET path configuration mode. To remove the setting of the SONET path overhead bytes from the configuration file and restore the system to its default condition, use the **no** form of this command.

overhead c2 *value*

no overhead c2 *value*

Syntax Description

Syntax Description

c2 *value*	Configures the C2 byte in the Path OverHead (POH) to indicate the contents of the payload inside the frame. C2 byte is to communicate the payload type that the SONET Framing OverHead (FOH) encapsulates.

Command Modes

Controller configuration

Command History

Release	Modification
XE 3.18SP	Support for this command was introduced on NCS 4200 Series.
XE Everest 16.5.1	This command was introduced on the Cisco ASR 920 Routers and Cisco NCS 4200 Series.

Usage Guidelines

This command is used to configure C2 flag as the path overhead.

Examples

The following example shows the configuration of C2 flag:

```
enable
configure terminal
controller MediaType 0/5/0
mode sonet
controller sonet 0/5/0
sts-1 1
overhead c2 10
end
```

Related Commands

Command	Description
controller sonet	Configures the SONET mode.
show controller sonet	Displays SONET controller configuration.

overhead j0

To specify the Regenerator Section (RS) Trace identifier (J0), use the **overheadj0** command in controller configuration mode. To restore the default value, use the **no** form of this command.

overhead j0 {**transmit** | **receive**} *string*
no overhead j0 {**transmit** | **receive**} *string*

Syntax Description

For NCS 4200 Series:

overhead j0 {*expected* | *tx*} [**length** *number* | **tracebuffer** *string*]

transmit	Specifies that the *string* argument is sent on the transmit line.
receive	Specifies that the configured *string* argument is matched with the string received from a peer.
string	Value in the range from 0 to 255 that is converted into character format and embedded in a 16-byte frame. The default is 1.
expected	Configures the expected trace identifier of the controller.
tx	Configures the packets transmitted.
length *number*	Specifies the length of the expected trace identifier.
tracebuffer *string*	Configures the SONET path trace buffer. Enters the ACSII text for the controller.

Command Default

The default value is 1, and no peer authentication is performed.

Command Modes

Controller configuration

Command History

Release	Modification
12.0(17)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T, and the **transmit** and **receive** keywords were added.
XE 3.18SP	Support for this command was introduced on NCS 4200 Series.

Usage Guidelines

RS trace is a maintenance feature of SONET. One byte (J0) of the Section overhead associated with each SONET frame is used to carry information identifying the transmitting equipment.

Use this command for peer authentication and continuity testing between two STM-1 optical peers. If the authentication string sent by the originating peer does not match the configured string on the receiving peer, the SONET controller will not come up on the receiving peer. Alarm logs on the originating peer will show that it has RS-Trace Identifier Mismatch (RS-TIM).

For NCS 4200 Series, use this command to configure line and section overhead of SONET line.

Examples

The following example shows how to configure J0 overhead in both the transmit and receive directions on a STM-1 trunk card:

```
Router(config)# controller sonet 2/0
Router(config-controller)# overhead j0 transmit 22
Router(config-controller)# overhead j0 receive 34
```

The following example shows how to set the RS Trace identifier to 82:

```
Router(config-controller)# overhead j0 transmit 82
```

Examples

For NCS 4200 Series, the following example shows how to configure line and section overhead:

```
enable
configure terminal
controller Mediatype 0/5/0
controller sonet 0/5/0
overhead j0 tx length 1-byte
end
```

Related Commands

Command	Description
controller sonet	Configures the SONET mode.
show controller sonet	Displays SONET controller configuration.

overhead j1

To configure the message length and the message text of the High Order Path Trace identifier (J1), use the **overheadj1** command in controller configuration or path configuration mode. To restore the default value, use the **no** form of this command.

overhead j1 length {**16** | **64**} {**transmit-message** | **receive-message**} *string*
no overhead j1 length {**16** | **64**} {**transmit-message** | **receive-message**} *string*

Syntax Description

For NCS 4200 Series, use the following command:

overhead j1 [**expected** | **tx**] [**length** | **message**]

length	Specifies the length of the authentication *string* argument.
16	Specifies that the length of the authentication *string*is 16 characters. The STM-1 trunk card supports a string length of 16.
64	Specifies that the length of the authentication *string*is 64 characters.
transmit-message	Specifies that the *string* argument is sent on the transmit line.
receive-message	Specifies that the configured *string* argument is matched with the string received from a peer.
string	Combination of characters and numbers for the specified **length** value.
tx	Configures the packets transmitted.
expected	Configures the expected trace identifier of the controller.

Command Default

The default message length is 16 for SDH framing and 64 for SONET framing. No peer authentication is performed.

Command Modes

Controller configuration

Path configuration

Command History

Release	Modification
12.0(17)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T, and the **transmit-message** and **receive-message** keywords were added.

Usage Guidelines

Path trace is a maintenance feature of SONET/SDH. One byte (J1) of the Path overhead associated with each path in the SONET/SDH frame is used to carry information identifying the originating Path Terminating Equipment (PTE).

Where you configure the Path Trace identifier depends on the framing (SDH or SONET) and the AUG mapping. In SDH with AU-4 mapping, the Path Trace identifier is configured at the SONET controller level. In SDH with AU-3 mapping or in SONET framing, the Path Trace identifier is configured at the path level.

In accordance with SONET and SDH standard requirements, the Path Trace message you enter is manipulated as follows:

- If you select a message length of 16, the actual message length can be up to 15 characters. An additional byte, prepended to the message, contains the result of a CRC7 calculated on the message. If the actual message text is fewer than 15 characters, the message text is padded to its full length with NULL characters.
- If you select a message length of 64 and the actual message text is fewer than 62 characters, the message text is padded with NULL characters. The last two byte positions, 63 and 64, are always CR/LF (0x0D/0x0A).

Use this command for peer authentication and continuity testing between two STM-1 optical peers. If the authentication string sent by the originating peer does not match the configured string on the receiving peer, the Path (and all E1 controllers within the path) will not come up on the receiving peer. Alarm logs on the originating peer will show that it has High Order Path-Trace Identifier Mismatch (HP-TIM).

Examples

The following example shows J1 configuration in SDH framing with AU-4 AUG mapping. The **overheadj1**command sets the message length to 16, and specifies the message text as metro_SF:

```
Router(config-controller)# au-4 1
Router(config-ctrlr-au4)# overhead j1 length 16 transmit-message metro_SF
```

The following example shows J1 configuration in SDH framing with AU-3 AUG mapping. The **overheadj1** command sets the message length to 16, and specifies the message text as metro_LA:

```
Router(config)# controller sonet 4/0Router(config-controller)# au-3 3
Router(config-ctrlr-au3)# overhead j1 length 16 receive-message metro_L
```

The following example shows J1 configuration in SONET framing in STS-1 mode. The **overheadj1** command sets the message length to 64, and specifies the message text:

```
Router(config)# controller sonet 4/0
Router(config-controller)# sts-1 3
Router(config-ctrlr-sts1)# overhead j1 length 64 transmit-message metro_washington
gsr_0057/4/3
```

The following example shows how to configure j1 overhead in both the transmit and receive directions:

```
Router(config)# controller sonet 2/0
Router(config-controller)# overhead j1 length 2 transmit-message 22
Router(config-controller)# overhead j1 length 2 receive-message 34
```

Examples

For NCS 4200 Series, the following example shows the configuration of J1 flag:

```
enable
configure terminal
controller sonet 0/5/0
sts-1 1
overhead j1 message word
end
```

overhead tunnel

To configure a transparent overhead tunnel on SDH or SONET controller, use the **overhead tunnel** command in the controller mode. To remove the tunnel from SDH or SONET controller, use the **no** form of this command.

For SONET

overhead tunnel {**all** | **sdcc** | **ldcc** | **k1k2** | **loh** | **soh** } **cem-group** *cem-id* **unframed**

For SDH

overhead tunnel {**all** | **ms-dcc** | **rs-dcc** | **k1k2** | **loh** | **soh** } **cem-group** *cem-id* **unframed**

Syntax Description

Syntax Description

all	Specify to include all section and line headers.
sdcc	Specify to include D1, D2, and D3 section header bytes for SONET.
ms-dcc	Specify to include D1, D2, and D3 section header bytes for SDH.
ldcc	Specify to include D4 to D12 line header bytes for SONET.
rs-dcc	Specify to include D4 to D12 line header bytes for SDH.
k1k2	Specify to include K1 and K2 line header bytes.
loh	Specify to include K1, K2, and D4 to D12, E2 line header bytes.
soh	Specify to include E1, F1, D1, D2, and D3 line header bytes.
cem-id	Specify CEM ID configured for the CEM group.

Command Default

None

Command Modes

Configuration mode

Command History

Release	Modification
Cisco IOS XE 16.9.x	Support for this command was introduced on ASR 900 Series.

Usage Guidelines

Before creating transparent overhead tunnel, ensure that you perform the following steps:

- Set mode under STS path before enabling overhead tunnel.
- Mode and TOH type should be same on both PEs in an end-to-end setup.

For more information on prerequisites for transparent overhead tunnel, see 1-Port OC-192 or 8-Port Low Rate CEM Interface Module Configuration Guide, Cisco IOS XE Everest 16.8.x (Cisco ASR 900 Series).

Examples

The following example shows how to configure transparent overhead tunnel on the SONET controller:

```
router(config)#controller sonet 0/7/7
```

```
router(config-controller)#overhead tunnel SDCC cem-group100 unframed
router(config-controller)#end
```

To configure transparent overhead tunnel pseudowire, use the following commands:

```
router(config)#interface cem 0/7/7
router(config-if)#cem  100
router(config-if)#xconnect  203.0.113.1  130  encapsulation MPLS
router(config-controller)#end
```

Related Commands

Command	Description
show cem circuit interface cem *interface-name*	Displays CEM interface configured for transparent overhead tunnel.

overhead s1s0

To set the SONET path overhead bytes in the frame header to a specific standards requirement or to ensure interoperability with equipment from another vendor, use the **overhead** command in SONET path configuration mode. To remove the setting of the SONET path overhead bytes from the configuration file and restore the system to its default condition, use the **no** form of this command.

overhead s1s0 *value*

no overhead s1s0 *value*

Syntax Description

Syntax Description

s1s0 *value*	Sets the SS bits value of the H1 byte in the SONET line overhead. For SONET mode, use 0 (this is the default).

Command Modes

Controller configuration

Command History

Release	Modification
XE 3.18SP	Support for this command was introduced on NCS 4200 Series.

Usage Guidelines

Use the **overhead** command to set the SONET overhead bytes in the frame header to a specific standards requirement. This command is used to configure line and section overhead.

Examples

The following example shows the configuration of overhead s1s0:

```
enable
configure terminal
controller MediaType 0/5/0
mode sonet
controller sonet 0/5/0
overhead s1s0 2
overhead j0 tx-length 1-byte
end
```

Related Commands

Command	Description
controller sonet	Configures the SONET mode.
show controller sonet	Displays SONET controller configuration.

password (satellite initial configuration)

To define or to change the password of the NM-1VSAT-GILAT network module required to enter satellite initial configuration mode, use the **password** command in the satellite initial configuration mode.

password *password*

Syntax Description

password	A string of up to 32 alphanumeric characters.

Command Default

The factory-supplied default password is active.

Command Modes

Satellite initial configuration.

Command History

Release	Modification
12.4(11)XJ2	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

The NM-1VSAT-GILAT network module has a factory-supplied unique default password to enter satellite initial configuration mode for initial configuration. During this configuration, the **password** command is used to set a user-defined password for subsequent entries to satellite initial configuration mode. The user-defined password consists of up to 32 alphanumeric characters.

Examples

The following example shows how to enter a user-defined password:

```
Router(sat-init-config)# password vsatuser
```

payload-compression

To enable payload compression, use the **payload-compression**command in CEM configuration mode. To disable payload compression, use the **no** form of this command.

payload-compression
no payload-compression

Syntax Description

This command has no arguments or keywords.

Command Default

Payload compression is disabled by default.

Command Modes

CEM configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

Payload compression can be enabled only for a maximum of 3 Mbps per network module.

Examples

The following example demonstrates how to enable payload compression.

```
Router(config-cem)# payload-compression
```

Related Commands

Command	Description
cem	Enters circuit emulation configuration mode.
payload-size	Configures payload size.
show cem	Displays CEM statistics.

payload-size dejitter-buffer

To configure the size of payload and dejitter-buffer of a circuit emulation (CEM) over MPLS, use the **payload-size dejitter-buffer** command in CEM configuration mode. To restore the default the size, use the **no** form of this command.

payload-size *size* **dejitter-buffer** *size*

no payload-size *size* **dejitter-buffer** *size*

size	The payload-size is the integer that defines the number of bytes per packet. Range of payload-size is from 64 to 1312. Range for dejitter-buffer size from 1 to 256 milliseconds. For T1, the valid values of payload size are 32 to 512. The default payload-size is 192 bytes and dejitter-buffer size is 5 milliseconds. For T3 clear channel, the default payload-size is 1024 bytes and dejitter-buffer size is 5 milliseconds. For T3 channelized, the default payload-size is 192 bytes and dejitter-buffer size is 5 milliseconds. For E1, the valid values of payload size are 64 to 1312. The default payload-size is 256 bytes and dejitter-buffer size is 5 milliseconds.

Command Default

The dejitter-buffer defaults to 5 milliseconds.

Command Modes

CEM configuration

Command History

Command History

Release	Modification
XE 3.18SP	This command was introduced.
XE Everest 16.5.1	This command was implemented on the Cisco ASR 900 Series Routers and Cisco NCS 4200 Series.

Usage Guidelines

Use this command to configure the size of each CEoIP packet. Smaller sizes reduce delay but diminish efficiency.

Note The payload size must be a multiple of the number of time slots and 16. The payload size you enter will automatically change to match the above requirement, and a console message will inform you the change. When you select a value of payload-size, the acceptable range of dejitter-buffer is displayed.

Examples

The following example shows how to set the payload size as 1024 and dejitter buffer to 10 milliseconds.

```
Router(config-controller)# payload-size 1024 dejitter-buffer 10
```

Related Commands

Command	Description
cem	Enters circuit emulation configuration mode.

payload-size

To configure the payload size of a circuit emulation (CEM) over IP (CEoIP) packet, use the **payload-size**command in CEM configuration mode. To restore the default payload size, use the **no** form of this command.

payload-size *size*
no payload-size

Syntax Description

size	Integer that defines the number of bytes per CEoIP packet. Range is from 1 to 1312. The maximum configurable payload size is as follows: • 1312 bytes if data protection is not enabled • 656 bytes if data protection is enabled The minimum configurable payload size for an unframed T1 or E1 channel is 256 bytes. The minimum configurable payload size for a framed T1 or E1 channel is as follows: • 56 bytes if the data rate is less than or equal to 256,000 kbps • 128 bytes if the data rate is greater than 256,000 kbps and less than or equal to 512,000 kbps • 256 bytes if the data rate is greater than 512,000 kbps The minimum configurable payload size for a serial channel is as follows: • 1 byte if the data rate is less than or equal to 2400 kbps • 4 bytes if the data rate is greater than 2400 kbps but less than or equal to 9600 kbps • 16 bytes if the data rate is greater than 9600 kbps but less than or equal to 32,000 kbps • 32 bytes if the data rate is greater than 32,000 kbps but less than or equal to 64,000 kbps • 64 bytes if the data rate is greater than 64,000 kbps but less than or equal to 256,000 kbps • 128 bytes if the data rate is greater than 256,000 kbps but less than or equal to 512,000 kbps • 256 bytes if the data rate is greater than 512,000 kbps **Note** For T1 and E1, the integer must be a multiple of the number of time slots and 16. For Cisco ASR 901 Series Aggregation Services Routers, the value specifies the size of the payload for packets on a structured CEM channel. Valid values are 32 to 512. The default payload size for a T1 channel is 192 bytes and for an E1 channel is 256 bytes. The default payload size is calculated by multiplying 8 by the number of timeslots and then multiplying the result by 1 ms packetization delay.

Command Default

The default payload size for a serial channel is 32 bytes. Defaults for T1 and E1 channels are shown in the tables below.

*Table 25: Default Payload Size for N*64-kbps T1/E1 Channels*

Number of Time Slots	Channel Data Rate (kbps)	Default Payload Size (bytes)
1	64	64
2	128	64
3	192	96
4	256	64
5	320	160
6	384	144
7	448	224
8	512	128
9	576	288
10	640	320
11	704	352
12	768	288
13	832	416
14	896	336
15	960	480
16	1024	256
Unframed T1	1544	512
Unframed E1	2048	512
17	1088	544
18	1152	576
19	1216	608
20	1280	560
21	1344	672
22	1408	528
23	1472	736
24	1536	528
25	1600	800

Number of Time Slots	Channel Data Rate (kbps)	Default Payload Size (bytes)
26	1664	624
27	1728	864
28	1792	560
29	1856	928
30	1920	720
31	1984	992

*Table 26: Default Payload Size for N*56-kbps T1 Channels*

Number of Time Slots	Channel Data Rate (kbps)	Default Payload Size (bytes)
1	56	56
2	112	56
3	168	168
4	224	56
5	280	280
6	336	168
7	392	168
8	448	168
9	504	504
10	560	280
11	616	616
12	672	336
13	728	728
14	784	280
15	840	840
16	896	336
17	952	952
18	1008	1008
19	1064	1064

Number of Time Slots	Channel Data Rate (kbps)	Default Payload Size (bytes)
20	1120	560
21	1176	672
22	1232	616
23	1288	1288
24	1344	672

Cisco ASR 901 Series Aggregation Services Routers

The default payload size for a structured CEM channel depends on the number of timeslots that constitute the channel.

Command Modes

- CEM configuration (config-if-cem)
- CEM circuit configuration (config-if-cem)

Command History

Release	Modification
15.1(2)SNG	This command was implemented on Cisco ASR 901 Series Aggregation Services Routers.
15.1(2)SNG	This command was implemented on Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Use this command to configure the size of each CEoIP packet. Smaller sizes reduce delay but diminish efficiency.

Note The payload size must be a multiple of the number of time slots and 16. The payload size entered by the user will be automatically changed to match the above requirement, and a console message will inform the user of this change.

The Cisco ASR 901 series router only supports a payload size of 486 (625 packets per second) or 243 (1250 packets per second).

Examples

The following example shows how to configure a payload size of 224.

```
Router(config-cem)# payload-size 224
```

Related Commands

Command	Description
cem	Enters circuit emulation configuration mode.
payload-compression	Enables payload compression.
payload-compression	Enables payload compression.

Command	Description
payload-compression	Enables payload compression.
show cem	Displays CEM channel statistics.

physical-interface

To create a physical subinterface and to associate it with the Virtual Multipoint Interface (VMI) on a router, use the **physical-interface** command in interface configuration mode. To return to the default mode, use the **no** form of this command.

physical-interface *interface-type / slot*
no physical-interface *interface-type / slot*

Syntax Description

interface-type	Type of interface or subinterface.
/ *slot*	Slot in which the interface is present.

Command Default

No physical interface exists.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(15)XF	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T to support VMIs in Mobile Adhoc Router-to-Radio Networks.
12.4(24)T	This command was modified. This command supports the subinterfaces and VLANS associated with an interface.

Usage Guidelines

The **physical-interface** command supports the subinterfaces and VLANs associated with an interface. This command also allows VMI interface to operate over encapsulated interfaces, if required. Only one physical interface can be assigned to a VMI interface. Because there is very high number of VMI interfaces that can be used, assign a new VMI for each physical interface.

Examples

The following example shows how to create a physical subinterface:

```
Router(config)# interface vmi1
Router(config-if)# physical-interface FastEthernet0/1
```

Related Commands

Command	Description
debug vmi	Displays debugging output for VMIs.
eigrp interface	Sets a threshold value to minimize hysteresis in a router-to-radio configuration.
interface vmi	Creates a VMI interface.
mode bypass	Enables VMIs to support multicast traffic

physical-layer

To specify the mode of a slow-speed serial interface on a router as either synchronous or asynchronous, use the **physical-layer** command in interface configuration mode. To return the interface to the default mode of synchronous, use the **no** form of this command.

physical-layer {**sync** | **async**}
no physical-layer

Syntax Description

sync	Places the interface in synchronous mode. This is the default.
async	Places the interface in asynchronous mode.

Command Default

Synchronous mode

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command applies only to low-speed serial interfaces available on Cisco 2520 through Cisco 2523 series routers.

In synchronous mode, low-speed serial interfaces support all interface configuration commands available for high-speed serial interfaces, except the following two commands:

- **half-duplex timer cts-delay**
- **half-duplex timer rts-timeout**

When placed in asynchronous mode, low-speed serial interfaces support all commands available for standard asynchronous interfaces.

When you enter this command, it does not appear in the output of **moresystem:running-config** and **morenvram:startup-config** commands because the command is a physical-layer command.

Examples

The following example shows how to change a low-speed serial interface from synchronous to asynchronous mode:

```
Router(config)# interface serial 2
Router(config-if)# physical-layer async
```

Related Commands

Command	Description
more	Displays a specified file.

platform console

To select the console that is used to access the virtual router interface, use the **platform console** command in global configuration mode.

platform console {**serial** | **virtual**}

Syntax Description

serial	Specifies that the virtual router is accessed using the virtual serial port on the ESXi host.
virtual	Specifies that the virtual router is accessed using the VMware VM console.

Command Default

No default.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 3.8S (Controlled Availability)	This command was introduced on the Cisco CSR 1000V Cloud Services Router.

Usage Guidelines

During the first-time installation and bootup of the virtual router, you choose whether to access the virtual router using the VM console or the virtual serial port on the ESXi host. The default setting is to use the VM console.

This command is used for changing the console access to the virtual router after first-time installation and bootup. After you enter the command, you must reload or power-cycle the router in order for the new setting to take effect.

Examples

The following example configures the virtual router to be accessed through the VM console:

```
Router> enable
Router# configure terminal
Router(config)# platform console virtual
Router(config)# end
Router# copy system:running-config nvram:startup-config
Router# reload
```

The following example configures the virtual router to be accessed through the virtual serial port:

```
Router> enable
Router# configure terminal
Router(config)# platform console serial
Router(config)# end
Router# copy system:running-config nvram:startup-config
Router# reload
```

platform cwan acl software-switched

To allow ACLs to be applied to packets that are software-switched between WAN cards and the route processor, use the **platformcwanaclsoftware-switched**command in global configuration mode. To have ACLs applied only to packets that are hardware-switched between WAN cards and the route processor, use the **no** form of this command.

platform cwan acl software-switched {**egress** | **ingress**}
no platform cwan acl software-switched {**egress** | **ingress**}

Syntax Description

egress	Allows ACLs to be applied to software-switched egress WAN packets.
ingress	Allows ACLs to be applied to software-switched ingress WAN packets.

Command Default

ACLs are not applied to packets that are software-switched between WAN cards and the route processor. ACLs are applied only to packets that are hardware-switched between WAN cards and the route processor.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
12.2(33)SXI2	This command was integrated into Cisco IOS Release 12.2(33)SXI2.

Usage Guidelines

By default, software-switched WAN packets are not subjected to ACL lookup in the ACL TCAM and are therefore not affected by hardware-only features. As a result, VACL capture will fail for software-switched WAN packets. The **platformcwanaclsoftware-switched**command allows ACLs to be applied to ingress or egress software-switched WAN packets.

When you use the **platformcwanaclsoftware-switched**command to allow VACL capture, these limitations apply:

Note The **platformcwanaclsoftware-switched**command is ignored by the SIP-600. Ingress software-switched packets on the SIP-600 are not subjected to ACL lookups, and VACL features are not supported.

Examples

This example shows how to enable ACLs for software-switched ingress WAN packets:

```
Router(config)#
platform cwan acl software-switched ingress
```

Related Commands

Command	Description
show platform acl software-switched	Displays whether ACLs are enabled for software-switched WAN packets.

platform enable controller mediaType

Use this command to to enable a particular license type on the controller port. Providing a particular license type is mandatory to enable the license on the IM.

platform enable controller Mediatype <*slot/bay/port*> <*port rate*>

Syntax Description

Syntax Description:

slot	Physical slot number of the interface
bay	Bay of the interface
port	Mediatype port number
port rate	Rate configured on the port

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
XE Everest 16.7.1	This command was integarted into the Cisco NCS 4200 Series, Cisco ASR 900 Series, and Cisco ASR 920 Routers.

Usage Guidelines

License enabling is allowed when the license with the same rate is configured on the port. The configuration fails if the license with a different rate is configured on the port.

Examples

The following example shows how to enable the license:

```
enable
configure terminal
platform enable controller MediaType 0/4/16 oc3
controller MediaType 0/4/16
mode sonet
exit
controller sonet 0/4/16
rate oc3
exit
```

Related Commands

Command	Description
show license detail	Verifies the license configuration.

platform hardware throughput crypto

To configure a throughput value on a physical router, use the **platform hardware throughput crypto** command in global configuration mode. To revert to the default value, use the **no** form of this command.

platform hardware throughput crypto { *throughput-value* }

no platform hardware throughput crypto

Syntax Description

throughput-value	Enter a throughput value. Use the question mark (?) online help function to display the available values. The available options vary depending on the device.

Command Default

The device-specific default throughput level is effective.

PID	Default Throughput
C8300-1N1S-4T2X	10 Mbps
C8300-2N2S-6T	10 Mbps
C8300-1N1S-6T	10 Mbps
C8300-2N2S-4T2X	10 Mbps
C8200-1N-4T	10 Mbps
C8200-1N-4T-L	10 Mbps
C8500-12X4QC	2.5 Gbps
C8500-12X	2.5 Gbps
C8500L-8S4X	2.5 Gbps
C8500-20X6C	T4

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.2	This command was introduced on Cisco Catalyst 8300, and 8500 Series Edge Platforms.
Cisco IOS XE Bengaluru 17.4.1	This command was introduced on the Cisco Catalyst 8200 Series Edge Platforms.

Usage Guidelines

Before you configure a throughput level, take note of these aspects:

- Ensure that you have configured a boot-level license. Otherwise **platform hardware throughput crypto** is not recognized as a valid command, on the command line interface. For information about configuring a boot-level license, see Configuring a Boot Level License.

- The throughput you are entitled to. This is a value that is represented in the License product ID (PID) when you order a Cisco DNA license. It can be a numeric throughput value, such as DNA-C-**10M**-E-3Y, or a tier-based throughput value, such as DNA-C-**T0**-E-3Y.

  Support for tier-based throughput configuration was introduced in Cisco IOS XE Cupertino 17.7.1a. Use the question mark (?) online help function to display the available tier-based *and* numeric throughput values. Refer to Tier and Numeric Throughput Mapping for Physical Platforms, Cisco IOS XE Cupertino 17.8.1a and Later Releases to know the numeric equivalent of a tier.

- If you are configuring throughput greater than 250 Mbps, ensure that you have installed a Smart Licensing Authorization Code (SLAC). Options greater than 250 Mbps are displayed only if SLAC is installed. For information about installing SLAC, see Manually Requesting and Auto-Installing a SLAC.

Support for aggregate throughput throttling was introduced in Cisco IOS XE Cupertino 17.8.1a. With this, when you configure throughput levels greater than 250 Mbps or Tier 2 and higher tiers on physical devices, aggregate throughput throttling is effective. *Aggregate throughput is double the bidirectional throughput*.

When aggregate throughput throttling is effective, throttling is not applied to transmitted (Tx) and received (Rx) traffic separately, rather, any ratio within the aggregate throughput limit applies. For example, If you configure a throughput of 500 Mbps on a device, a maximum of 1 Gbps transmitted (Tx) traffic and 0 Mbps received (Rx) traffic, or, 100 Mbps Tx and 900 Mbps Rx, or any other ratio within the aggregate 1 Gbps throughput limit, is supported. For more information and examples, see Throughput as a Numeric Value and Throughput as a Tier.

To display throughput information, enter the **show platform hardware throughput crypto** command in privileged EXEC mode.

The following example shows you how to configure a tier-based throughput value.

Displaying current configuration:

```
Device# show platform hardware throughput crypto
show platform hardware throughput crypto
Current configured crypto throughput level: 250M
     Level is saved, reboot is not required
Current enforced crypto throughput level: 250M
Crypto Throughput is throttled at 250M
Default Crypto throughput level: 10M
Current boot level is network-premier
```

Verifying SLAC is installed before configuring a throughput level greater than 250 Mbps or Tier 2 and higher tiers:

```
Device# show license authorization
Overall status:
  Active: PID:C8300-2N2S-4T2X,SN:FDO2250A0J5
      Status: SMART AUTHORIZATION INSTALLED on Mar 02 05:05:19 2022 UTC
      Last Confirmation code: 418b11b3

Authorizations:
  Router US Export Lic. for DNA (DNA_HSEC):
    Description: U.S. Export Restriction Compliance license for
    DNA based Routers
    Total available count: 1
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:C8300-1N1S-4T2X,SN:FDO2250A0J5
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
          Term Count: 1
```

```
Purchased Licenses:
  No Purchase Information Available
```

Configuring a tier-based throughput value from the list of available values for this device:

```
Device# configure terminal
Device(config)# platform hardware throughput crypto ?
  100M  100 mbps bidirectional thput
  10M   10 mbps bidirectional thput
  15M   15 mbps bidirectional thput
  1G    2 gbps aggregate thput
  2.5G  5 gbps aggregate thput
  250M  250 mbps bidirectional thput
  25M   25 mbps bidirectional thput
  500M  1gbps aggregate thput
  50M   50 mbps bidirectional thput
  T0    T0(up to 15 mbps) bidirectional thput
  T1    T1(up to 100 mbps) bidirectional thput
  T2    T2(up to 2 gbps) aggregate thput
  T3    T3(up to 5 gbps) aggregate thput

Device(config)# platform hardware throughput crypto T2
% These values don't take effect until the next reboot.
Please save the configuration.
*Mar 02 05:06:19.042: %CRYPTO_SL_TP_LEVELS-6-SAVE_CONFIG_AND_RELOAD:
New throughput level not applied until reload; please save config
```

Saving configuration to ensure changes persist across reloads and reloading the device:

```
Device# exit
Device# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Device# reload
Proceed with reload? [confirm]
*Mar 02 05:07:00.979: %SYS-5-RELOAD: Reload requested by console.
Reload Reason: Reload Command.
```

Displaying configuration again:

```
Device# show platform hardware throughput crypto
Current configured crypto throughput level: T2
     Level is saved, reboot is not required
Current enforced crypto throughput level: 1G
Crypto Throughput is throttled at 2G(Aggregate)
Default Crypto throughput level: 10M
Current boot level is network-premier
```

Related Commands

Command	Description
show platform hardware throughput crypto	Displays throughput information on a physical router.

platform hardware throughput level

To change the maximum throughput level on the virtual router, use the **platform hardware throughput level** command in global configuration mode. To return the platform throughput level to the default value, use the **no** form of this command.

Cisco IOS XE Release 3.9S:

platform hardware throughput level {**10000** | **25000** | **50000** | **eval-only**}

Cisco IOS XE Release 3.10S and Later:

platform hardware throughput level MB {**10** | **100** | **1000** | **25** | **250** | **50** | **500**}

Syntax Description

Cisco IOS XE Release 3.9S:	
10000	Sets the maximum throughput to 10,000 Kbps (10 Mbps).
25000	Sets the maximum throughput to 25,000 Kbps (25 Mbps).
50000	Sets the maximum throughput to 50,000 Kbps (50 Mbps).
eval-only	Specifies to use the maximum throughput for the evaluation license only.
Cisco IOS XE Release 3.10S:	
10	Sets the maximum throughput to 10 Mbps.
100	Sets the maximum throughput to 100 Mbps.
1000	Sets the maximum throughput to 1 Gbps.
25	Sets the maximum throughput to 25 Mbps.
250	Sets the maximum throughput to 250 Mbps.
50	Sets the maximum throughput to 50 Mbps.
500	Sets the maximum throughput to 500 Mbps.

Command Default

The default maximum throughput level is determined by the installed base license.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced on the Cisco CSR 1000V Series Cloud Services Router.
Cisco IOS XE 3.10S	The command was updated to change the keywords to units in Mbps, and support for maximum throughput values of 100 Mbps, 250 Mbps, 500 Mbps, and 1 Gbps was added.

Usage Guidelines

The Cisco CSR 1000V requires the installation of base licenses that set the maximum throughput of the platform.

Depending on the configuration and the licenses installed, you may need to manually increase or decrease the maximum throughput level on the Cisco CSR 1000V. The maximum throughput on the router before the license is activated, or if the license is invalidated, is 2.5 Mbps. When you install the base subscription license and accept the EULA, the maximum throughput on the Cisco CSR 1000V will increase to the level allowed by the license.

You may need to manually change the maximum throughput level in the following cases:

- If you are using an evaluation license. When the evaluation license is first installed, the maximum throughput is limited to 2.5 Mbps before the license is activated. You must accept the EULA and enter the **platform hardware throughput level**command to increase the maximum throughput. When the 60-day evaluation license expires, the maximum throughput level reverts to 2.5 Mbps.
- If you want to reduce the maximum throughput level from the maximum permitted by the installed licenses. For example, if you have the 50-Mbps license installed and you want to reduce the maximum throughput to 25 Mbps. You must enter the **platform hardware throughput level** command to reduce the maximum throughput.
- If you previously changed the maximum throughput using the **platform hardware throughput level** command. When you enter the command, it becomes part of the configuration file. You must enter the command again to change the maximum throughput level.

When changing the maximum throughput level, you do not need to reboot the Cisco CSR 1000V for the change to take effect. If you try to increase the throughput level higher than what the installed license supports, you will receive an error message.

Example

The following example changes the maximum throughput level to 500 Mbps:

```
Router(config)# platform hardware throughput level MB 500
```

The following example changes the maximum throughput level to the default level supported by the installed license:

```
Router(config)# no platform hardware throughput level
```

Related Commands

Command	Description
show platform hardware throughput level	Displays the current maximum throughput level for a virtual router.

platform ip features sequential

To enable Internet Protocol (IP) precedence-based or differentiated services code point (DSCP)-based egress quality of service (QoS) filtering to use any IP precedence or DSCP policing or marking changes made by ingress policy feature card (PFC) QoS, use the **platformipfeaturessequential** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

platform ip features sequential [**access-group** {*ip-acl-nameip-acl-number*}]
no platform ip features sequential [**access-group** {*ip-acl-nameip-acl-number*}]

Syntax Description

access-group *ip-acl-name*	(Optional) Specifies the name of the ACL that is used to specify the match criteria for the recirculation packets.
access-group *ip-acl-number*	(Optional) Specifies the number of the ACL that is used to specify the match criteria for the recirculation packets; valid values are from 1 to 199 and from 1300 to 2699.

Command Default

IP precedence-based or DSCP-based egress QoS filtering uses received IP precedence or DSCP values and does not use any IP precedence or DSCP changes made by ingress QoS as the result of policing or marking.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Caution If the switch is operating in PFC3A mode with egress ACL support for remarked DSCP configured, when the PFC3 processes traffic to apply ingress PFC QoS, it applies ingress PFC QoS filtering and ingress PFC QoS, and incorrectly applies any egress QoS filtering and egress PFC QoS configured on the ingress interface, which results in unexpected behavior if QoS filtering is configured on an interface where egress ACL support for remarked DSCP is enabled. This problem does not occur in other PFC3 modes.

The enhanced egress-QoS filtering enables the IP precedence-based or DSCP-based egress-QoS filtering to use any IP precedence or DSCP policing or marking changes made by ingress QoS.

The nonenhanced egress-QoS filtering behavior is the normal Cisco 7600 series router or the Catalyst 6500 series switch behavior when QoS is applied in the hardware.

The PFC3 provides egress PFC QoS only for Layer 3-switched and routed traffic on egress Layer 3 interfaces (either LAN ports configured as Layer 3 interfaces or VLAN interfaces).

You configure enhanced egress QoS filtering on ingress Layer 3 interfaces (either LAN ports configured as Layer 3 interfaces or VLAN interfaces).

To enable enhanced egress QoS filtering only for the traffic filtered by a specific standard, extended named, or extended numbered IP ACL, enter the IP ACL name or number.

If you do not enter an IP ACL name or number, enhanced egress QoS filtering is enabled for all IP ingress IP traffic on the interface.

Note When you configure enhanced egress-QoS filtering, the PFC3A processes traffic to apply ingress PFC QoS. The PFC3A applies ingress-QoS filtering and Cisco 7600 series router or the Catalyst 6500 series switch hardware ingress QoS. The PFC3A incorrectly applies any egress-QoS filtering and Cisco 7600 series router or the Catalyst 6500 series switch hardware egress QoS that is configured on the ingress interface.

Note If you configure enhanced egress-QoS filtering on an interface that uses Layer 2 features to match the IP precedence or DSCP as modified by ingress-QoS marking, the packets are redirected or dropped and prevented from being processed by egress QoS.

Note If you enable enhanced egress-QoS filtering, the hardware acceleration of NetFlow-based features such as reflexive ACL, NAT, and TCP intercept are disabled.

To verify configuration, use the **showrunning-configinterface** command.

Examples

The following example shows how to enable enhanced egress-QoS filtering:

```
Router(config-if)# platform ip features sequential

Router(config-if)#
```

The following example shows how to disable enhanced egress-QoS filtering:

```
Router(config-if)# no platform ip features sequential

Router(config-if)#
```

Related Commands

Command	Description
show running-config interface	Displays the contents of the currently running configuration file.

platform punt-keepalive

To enable the Punt-Keepalive feature and monitor the status of the punt path between the forwarding processor (FP) and the route processor (RP), use the **platform punt-keepalive** command in the global configuration mode. To disable the Punt-Keepalive feature, use the **no** form of this command.

platform punt-keepalive{**disable-kernel-core** | **settings**{**fatal-count** *fatal-count* | **transmit-interval** *transmit-interval* | **warning-count** *warning-count*}}

no platform punt-keepalive

Syntax Description

disable-kernel-core	Disables Linux kernel crash generation and IOS Daemon (IOSD) crash generation.
settings	Specifies the keepalive parameters.
fatal-count *fatal-count*	Specifies the upper limit of consecutive keepalive warnings for triggering system failures. The range is from 15 to 60. Linux kernel crash generation and IOSD crash generation occur when the fatal count reaches the upper limit.
transmit-interval *transmit-interval*	Specifies the keepalive transmit interval, in seconds. The range is from 2 to 30. The default is 2.
warning-count *warning-count*	Specifies the upper limit of consecutive keepalive message failures for reporting warnings. The range is from 10 to 60. Linux kernel crash generation and IOSD crash generation occur when the warnings reach the upper limit.

Command Default

The Punt-Keepalive feature is enabled, and the Kernel core crash and IOSD crash generation are enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.

Usage Guidelines

The **platform punt-keepalive** command is available only if all the following conditions are met:

- Device is in an active state.
- FP is present and is online.
- System reload is not in progress.

The punt-keepalive process checks the status of the device and the FP every 30 seconds. However, when the status for the device changes from standby to active, or when the FP goes online, the device waits for another 30 seconds before sending the first keepalive message. Disabling the Linux kernel crash generation and IOS Daemon (IOSD) crash generation allows the system to settle down after the occurrence of critical events.

IOSD or Kernel driver code can cause a keepalive failure; a keepalive failure can force IOSD crash generation and Linux kernel crash generation. The crash generation type depends on the chassis and the operating mode. The following table describes the relationship between chassis, operation mode, and type of crash generation.

Table 27: Relationship Between Chassis, Operation Mode, and Type of Crash Generation

Chassis	Operation Mode	Redundancy Status	Type of Crash Generation
Cisco ASR 1002 Cisco ASR 1002-F	Single IOSD	-	IOSD core Kernel core
Cisco ASR 1001 ASR 1004	Dual IOSD	Not Hot	IOSD core Kernel core
IOSD core Kernel core	Dual IOSD	Hot	IOSD core
Cisco ASR 1006 Cisco ASR 1013	Single or Dual RP	Any	IOSD core Kernel core

Kernel core crash generation takes approximately five minutes. Disable kernel core crash generation for a faster reboot of the system.

Examples

The following example shows how to disable kernel core crash generation and IOSD crash generation by using the **platform punt-keepalive** command:

```
Device(config)# platform punt-keepalive disable-kernel-core
```

Related Commands

Command	Description
show platform software infrastructure punt-keepalive	Displays information about **platform punt-keepalive** command settings.

platform punt-arp-unicast cpu-queue-host

To punt ARP unicast packets through the Routing protocol queue, when packets are forwarded between the forwarding processor (FP) and the route processor (RP), use the **platform punt-arp-unicast cpu-queue-host** command in the global configuration mode. To punt ARP unicast packets through the Broadcast queue, use the **no** form of this command.

Note This command is supported on Cisco IOS XE ASR 920 platforms.

platform punt-arp-unicast cpu-queue-host

no platform punt-arp-unicast cpu-queue-host

Command Default

The platform punt-arp-unicast feature is not enabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.10.1	This command was modified.

platform scp retry interval

To enable Switch-Module Configuration Protocol (SCP) fast retry and set the fast-retry interval, use the **platformscpretryinterval** command in global configuration mode. To disable SCP fast retry, use the **no** form of this command.

platform scp retry interval *timeout-value*
no platform scp retry interval

Syntax Description

timeout-value	Fast retry interval; valid values are from 200 to 2000 milliseconds.

Command Default

2000 milliseconds

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Note Use this command under the direction of the Cisco TAC only.

Examples

This example shows how to enable SCP fast retry and set the fast-retry interval:

```
Router(config)# platform scp retry interval 600
Router(config)#
```

platform smart-sfp

To configure the Gigabit Ethernet or TenGig Ethernet as VCoP smart SFP on OC3 or OC12 or DS3 mode, use the **platform smart-sfp interface** command in SONET/PDH configuration mode. To remove the VCoP smart SFP, use the **no** form of this command.

platform smart-sfp interface gig/tengig*slot/bay/port* **type***OC3/OC12/DS3*

no platform smart-sfp

Syntax Description

Syntax Description

platform	Specifies a platform keyword.
smart sfp	Specifies a smart sfp keyword. SFP stands for Small Form-Factor Pluggable.
interface	Specifies a interface keyword.
gig/tengig	Specifies the Gigabit Ethernet or TenGig Ethernet port where VCoP is inserted.
slot	Slot number of the controller. A forward slash mark (/) is required between the slot argument and the bay argument.
bay	Bay number of the controller. A forward slash mark (/) is required.
port	Port number of the controller. A forward slash mark (/) is required between the bay argument and the port argument.
type	Type of the interface to be configured. The interface type can be OC3/OC12/ DS3.

Command Modes

Global configuration

Command History

Release	Modification
XE 3.18SP	Support for this command was introduced on the Cisco NCS 4200 Series.
XE Everest 16.5.1	This command was introduced to support DS3 mode of VCoP Smart SFP for Cisco NCS 4200 Series and Cisco ASR 920 Routers.

Usage Guidelines

This command is used to identify the VCoP OC-n/DS3 smart SFP inserted in the Cisco NCS 4200 Series. This command is used to configure VCoP OC-n smart SFP type i.e. OC3 or OC12 and DS3 mode. Before executing this command for a particular port, the configuration on that port must be deleted or set as default.

This command sets the Gig port as the smart SFP port for configuring the CEP for the given port number.

Examples

The following example shows how to configure VCoP smart SFP on Gig and TenGig ports.

Configruing VCoP smart SFP on OC3 mode

For Gigabit port:

```
Router(config)# configure terminal
Router(config)# platform smart-sfp interface GigabitEthernet 0/0/8 type OC-3
```

For TenGig port:

```
Router(config)# configure terminal
Router(config)# platform smart-sfp interface TenGig 0/0/8 type OC-3
```

Configruing VCoP smart SFP on OC12 mode

For Gigabit port:

```
Router(config)# configure terminal
Router(config)# platform smart-sfp interface GigabitEthernet 0/0/8 type OC-12
```

For TenGig port:

```
Router(config)# configure terminal
Router(config)# platform smart-sfp interface TenGig 0/0/8 type OC-12
```

Configruing VCoP smart SFP on T3 mode

For Gigabit port:

```
Router(config)# configure terminal
Router(config)# platform smart-sfp interface GigabitEthernet 0/0/8 type ds3
```

For TenGig port:

```
Router(config)# configure terminal
Router(config)# platform smart-sfp interface TenGig 0/0/8 type ds3
```

Related Commands

Command	Description
show cem circuit	Displays the circuit emulation (CEM) statistics for the configured CEM circuits.
show controller	Displays SONET/T3 controller configuration.

platform time-source

To initiate Time of Day (ToD) synchronization on a line card, use the **platformtime-source** command in global configuration mode. To disable the platform time-source, use the **no** form of this command.

platform time-source {**ntp** | **ptp**}
no platform time-source

Syntax Description

ntp	Configures Network Time Protocol (NTP) clock source
ptp	Configures Precision Time Protocol (PTP) clock source

Command Default

The **platformtime-source** command is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
15.1(2)S	This command was introduced on the Cisco 7600 routers.
Cisco IOS XE Release 3.12	This command is integrated on the Cisco ASR 900 Series Routers. The **ptp** keyword is not supported on the Cisco ASR 900 Series Routers.

Usage Guidelines

Cisco 7600 Router

Either the 2-Port Gigabit Synchronous Ethernet SPA (PTP) or NTP module on the Route Processor is used to initiate the ToD synchroniztion. The NTP ToD information is converted into PTP format and then synchronized to all the ES+ Linecards.

Cisco ASR 900 Series Routers

This command is used to enable or disable NTP clock (Time of Day) synchronization on the ethernet ports. The ports will use NTP ToD value to timestamp Y.1731 DM packets.

Example

This example shows how to configure platform time-source on the Cisco ASR 900 Series Router.

```
Router (config)# platform time-source ntp
```

Examples

This example shows how to configure the platform time-source on the Cisco 7600 Router.

```
Router (config)#platform time-source ptp 1 master top 6/0/2 slave lo0
or
Router (config)#platform time-source ntp
```

Related Commands

Command	Description
show platform time-source	This command displays the configuration details of the platform time-source.

platform trace boottime process forwarding-manager module interfaces

To enable Forwarding Manager Route Processor and Embedded Service Processor trace messages for the RP forwarding manager process during bootup, use the **platformtraceboottimeprocessforwarding-managermoduleinterfaces**command in the Global configuration mode. To disable debug messages, use the **no** form of this command.

platform trace boottime slot *slot* **bay** *bay* **process forwarding-manager module interfaces level** *level*
no platform trace boottime slot *slot* **bay** *bay* **process forwarding-manager module interfaces**

Syntax Description

slot	Shared Port Adapter (SPA) Interprocessor, Embedded Service Processor or Route Processor slot. Valid options are: • *R0* --Route Processor slot 0 • *R1* --Route Processor slot 1
bay	Chassis bay to be configured. Valid options are: • *0* • *1*
level *level*	Selects the trace level. The trace level determines the amount of information that is to be stored about a module in the trace buffer or file. Valid options are: • **max** --Provides the maximum possible message. • **notice messages** --Provides notice messages.

Command Default

The default tracing level for every module on the Cisco ASR 1000 Series Routers is Notice.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Routers.

Usage Guidelines

Trace-level settings are leveled that is every setting contains all the messages from the lower setting plus the messages from its own setting. For instance, setting the trace level to 3 (error) ensures that the trace file contains all the output for the 0 (emergencies), 1 (alerts), 2 (critical), and 3 (error) settings. Setting the trace level to 4 (warning) ensures that all the trace output for a specific module is included in that trace file.

All trace levels cannot be configured by users. Specifically, the alert, critical, and notice tracing levels cannot be set by users. To trace these messages, set the trace level to a higher level, which collects these messages.

When setting the trace levels, it is also important to remember that the setting is not done in a configuration mode. As a result of this, trace level settings are returned to their defaults after every router reload.

Caution Setting tracing of a module to the debug level or higher can have a negative performance impact. Setting tracing to the debug level or higher should be done with discretion.

Caution Setting a large number of modules to high tracing levels can severely degrade performance. If a high level of tracing is needed in a specific context, it is almost always preferable to set a single module on a higher tracing level rather than setting multiple modules to high tracing levels.

Examples

In the following example, the trace level for the forwarding processor module in the Forwarding Manager of the ESP processor in slot R0 is set to the informational tracing level (max):

```
Router(config)# platform trace boottime slot R0 bay 1 process forwarding-manager
forwarding-manager level max
```

Related Commands

Command	Description
show platform software trace level	Displays trace levels for specified modules.
show platform software trace message	Displays trace messages.

pm fec threshold

To configure performance monitoring thresholds on the FEC layer, use the **pmfecthreshold**command in DWDM configuration mode. To disable the performance monitoring threshold, use the **no** form of this command.

pm {**15-min** | **24-hour**} **fec** **threshold** {**ec-bits** | **uc-words**} *threshold*
nopm {**15-min** | **24-hour**} **fec** **threshold** {**ec-bits** | **uc-words**} *threshold*

Syntax Description

15-min	Configures the performance monitoring thresholds for 15-minute intervals.
24-hour	Configures performance monitoring thresholds for 24-hour intervals.
ec-bits	Bit errors corrected (BIEC). Indicates the number of bit errors corrected in the DWDM trunk line during the performance monitoring time interval.
uc-words	Uncorrectable Words. Indicates the number of uncorrectable words detected in the DWDM trunk line during the performance monitoring time interval.
threshold	Threshold for the performance monitoring parameter.

Command Default

No threshold is configured.

Command Modes

DWDM configuration.

Command History

Release	Modification
15.1(3)S	This command was introduced on the Cisco 7600 series routers.

Examples

The following example shows how to configure an FEC layer performance monitoring threshold for uncorrectable words:

```
Router(config)# controller dwdm 0/0
Router(config-controller)# pm 15-min fec threshold uc-words 900 enable
```

Related Commands

Command	Description
show controller dwdm pm fec	Displays performance measurement information for the FEC layer.

pm optics report

To enable threshold crossing alert (TCA) generation on the optics layer, use the **pmopticsreport**command in DWDM configuration mode. To disable TCA reporting, use the **no** form of this command.

pm {**15-min** | **24-hour**} **optics report** {**lbc** | **opr** | **opt**} {**max-tca** | **min-tca**} **enable**
nopm {**15-min** | **24-hour**} **optics report** {**lbc** | **opr** | **opt**} {**max-tca** | **min-tca**} **enable**

Syntax Description

15-min	Configures TCA generation for 15-minute intervals.
24-hour	Configures TCA generation for 24-hour intervals.
lbc	Laser bias current.
opr	Optical power on the unidirectional port.
opt	Transmit optical power in dBm.
max-tca	Indicates that the maximum value of the parameter is compared against the threshold to determine if a TCA should be generated.
min-tca	Indicates that the minimum value of the parameter is compared against the threshold to determine if a TCA should be generated.
enable	Enables TCA generation for the specified parameter on the DWDM controller.

Command Default

TCA reporting is not enabled.

Command Modes

DWDM configuration.

Command History

Release	Modification
15.1(3)S	This command was introduced on the Cisco 7600 series routers.

Examples

The following example shows how to enable TCA reporting on the optics layer reporting for the maximum OPT:

```
Router(config)# controller dwdm 0/0
Router(config-controller)# pm 15-min optics report opt max-tca enable
```

Related Commands

Command	Description
show controller dwdm pm optics	Displays performance measurement information for the optics layer.

pm otn report

To enable threshold crossing alert (TCA) generation on the optical transport network (OTN) layer, use the **pmotnreport**command in DWDM configuration mode. To disable TCA reporting, use the **no** form of this command.

pm {**15-min** | **24-hour**} **otn** **report** *otn-parameter* **enable**
nopm {**15-min** | **24-hour**} **otn** **report** *otn-parameter* **enable**

Syntax Description

15-min	Configures TCA generation for 15-minute intervals.
24-hour	Configures TCA generation for 24-hour intervals.
otn-parameter	Specific parameter for which to configure the threshold. OTN parameters can be as follows: • **bbe-pm-fe** --Far-end path monitoring background block errors (BBE-PM). Indicates the number of background block errors recorded in the optical transport network (OTN) path during the performance monitoring time interval. • **bbe-pm-ne** --Near-end path monitoring background block errors (BBE-PM). • **bbe-sm-fe** --Far-end section monitoring background block errors (BBE-SM). Indicates the number of background block errors recorded in the OTN section during the performance monitoring time interval. • **bbe-sm-ne** --Near-end section monitoring background block errors (BBE-SM). • **bber-pm-fe** --Far-end path monitoring background block errors ratio (BBER-PM). Indicates the background block errors ratio recorded in the OTN path during the performance monitoring time interval. • **bber-pm-ne** --Near-end path monitoring background block errors ratio (BBER-PM). • **bber-sm-fe** --Far-end section monitoring background block errors ratio (BBER-SM). Indicates the background block errors ratio recorded in the OTN section during the performance monitoring time interval. • **bber-sm-ne** --Near-end section monitoring background block errors ratio (BBER-SM) • **es-pm-fe** --Far-end path monitoring errored seconds (ES-PM). Indicates the errored seconds recorded in the OTN path during the performance monitoring time interval. • **es-pm-ne** --Near-end path monitoring errored seconds (ES-PM). • **es-sm-fe** --Far-end section monitoring errored seconds (ES-SM). Indicates the errored seconds recorded in the OTN section during the performance monitoring time interval. • **es-sm-ne** --Near-end section monitoring errored seconds (ES-SM). • **esr-pm-fe** --Far-end path monitoring errored seconds ratio (ESR-PM). Indicates the errored seconds ratio recorded in the OTN path during the performance monitoring time interval.

	• **esr-pm-ne** --Near-end path monitoring errored seconds ratio (ESR-PM). • **esr-sm-fe** --Far-end section monitoring errored seconds ratio (ESR-SM). Indicates the errored seconds ratio recorded in the OTN section during the performance monitoring time interval. • **esr-sm-ne** --Near-end section monitoring errored seconds ratio (ESR-SM). • **fc-pm-fe** --Far-end path monitoring failure counts (FC-PM). Indicates the failure counts recorded in the OTN path during the performance monitoring time interval. • **fc-pm-ne** --Near-end path monitoring failure counts (FC-PM). • **fc-sm-fe** --Far-end section monitoring failure counts (FC-SM). Indicates the failure counts recorded in the OTN section during the performance monitoring time interval. • **fc-sm-ne** --Near-end section monitoring failure counts (FC-SM). • **ses-pm-fe** --Far-end path monitoring severely errored seconds (SES-PM). Indicates the severely errored seconds recorded in the OTN path during the performance monitoring time interval. • **ses-pm-ne** --Far-end path monitoring severely errored seconds (SES-PM). • **ses-sm-fe** --Far-end section monitoring severely errored seconds (SES-SM). Indicates the severely errored seconds recorded in the OTN section during the performance monitoring time interval. • **ses-sm-ne** --Near-end section monitoring severely errored seconds (SES-SM). • **sesr-pm-fe** --Far-end path monitoring severely errored seconds ratio (SESR-PM). Indicates the severely errored seconds ratio recorded in the OTN path during the performance monitoring time interval. • **sesr-pm-ne** --Near-end path monitoring severely errored seconds ratio (SESR-PM). • **sesr-sm-fe** --Far-end section monitoring severely errored seconds ratio (SESR-SM). Indicates the severely errored seconds ratio recorded in the OTN section during the performance monitoring time interval. • **sesr-sm-ne** --Near-end section monitoring severely errored seconds ratio (SESR-SM). • **uas-pm-fe** --Far-end path monitoring unavailable seconds (UAS-PM). Indicates the unavailable seconds recorded in the OTN path during the performance monitoring time interval. • **uas-pm-ne** --Near-end path monitoring unavailable seconds (UAS-PM). • **uas-sm-fe** --Far-end section monitoring unavailable seconds (UAS-SM). Indicates the unavailable seconds recorded in the OTN section during the performance monitoring time interval. • **uas-sm-ne** --Near-end section monitoring unavailable seconds (UAS-SM).
enable	Enables TCA generation for the specified parameter on the DWDM controller.

Command Default

TCA generation is not enabled.

Command Modes

DWDM configuration.

Command History

Release	Modification
15.1(3)S	This command was introduced on the Cisco 7600 series routers.

Examples

The following example shows how to enable TCA generation on the OTN layer reporting for the path monitoring errored seconds ratio (ESR-PM):

```
Router(config)# controller dwdm 0/0
Router(config-controller)# pm 15-min otn report esr-pm-fe enable
```

Related Commands

Command	Description
show controller dwdm pm otn	Displays performance measurement information for the OTN layer.

pm optics threshold

To configure performance monitoring thresholds on the optics layer, use the **pmopticsthreshold**command in DWDM configuration mode. To disable the performance monitoring threshold, use the **no** form of this command.

pm {**15-min** | **24-hour**} **optics threshold** {**lbc** | **opr** | **opt**} {**max** | **min**} *threshold*
nopm {**15-min** | **24-hour**} **optics threshold** {**lbc** | **opr** | **opt**} {**max** | **min**} *threshold*

Syntax Description

15-min	Configures performance monitoring thresholds for 15-minute intervals.
24-hour	Configures performance monitoring thresholds for 24-hour intervals.
lbc	Laser bias current.
opr	Optical power on the unidirectional port.
opt	Transmits optical power in dBm.
max	Indicates that the *threshold* is for the maximum value of the parameter.
min	Indicates that the *threshold* is for the minimum value of the parameter.
threshold	Threshold for the performance monitoring parameter.

Command Default

No thresholds are configured.

Command Modes

DWDM configuration.

Command History

Release	Modification
15.1(3)S	This command was introduced on the Cisco 7600 series routers.

Examples

The following example shows how to configure an optics layer performance monitoring threshold for maximum OPT:

```
Router(config)# controller dwdm 0/0
Router(config-controller)# pm 15-min optics threshold opt max 700
```

Related Commands

Command	Description
show controller dwdm pm optics	Displays performance measurement information for the optics layer.

pm otn threshold

To configure performance monitoring thresholds on the optical transport network (OTN) layer, use the **pmotnthreshold**command in DWDM configuration mode. To disable TCA reporting, use the **no** form of this command.

pm {**15-min** | **24-hour**} **otn** **threshold** *otn-parameter* *threshold*
nopm {**15-min** | **24-hour**} **otn** **threshold** *otn-parameter* *threshold*

Syntax Description

15-min	Configures performance monitoring thresholds for 15-minute intervals.
24-hour	Configures performance monitoring thresholds for 24-hour intervals.
otn-parameter	Specific parameter for which to configure the threshold. OTN parameters can be as described in the **pmotnreport** command.
threshold	Threshold for the performance monitoring parameter.

Command Default

No thresholds are configured.

Command Modes

DWDM configuration.

Command History

Release	Modification
15.1(3)S	This command was introduced on the Cisco 7600 series routers.

Examples

The following example shows how to configure an OTN layer performance monitoring threshold for path monitoring errored seconds ratio (ESR-PM):

```
Router(config)# controller dwdm 0/0
Router(config-controller)# pm 15-min otn threshold esr-pm-ne 800
```

Related Commands

Command	Description
show controller dwdm pm otn	Displays performance measurement information for the OTN layer.

port (interface)

To enable an interface on a PA-4R-DTR port adapter to operate as a concentrator port, use the **port**command in interface configuration mode. To restore the default station mode, use the **no** form of this command.

port
no port

Syntax Description

This command has no arguments or keywords.

Command Default

Station mode

Command Modes

Interface configuration

Command History

Release	Modification
11.3(3)T	This command was introduced.

Usage Guidelines

By default, the interfaces of the PA-4R-DTR operate as Token Ring stations. Station mode is the typical operating mode. Use this command to enable an interface to operate as a concentrator port.

Examples

The following example configures the PA-4R-DTR ports to operate in concentrator mode on a Cisco 7000 series router:

```
Router(config)# interface tokenring 3/0/0
Router(config-if)# port
```

port access-map

To create a port access map or enter port access-map command mode, use the **portaccess-map** command in global configuration mode. To remove a mapping sequence or the entire map, use the **no** form of this command.

port access-map *name* [*seq#*]
no port access-map *name* [*seq#*]

Syntax Description

name	Port access-map tag.
seq#	(Optional) Map sequence number; valid values are 0 to 65535.

Command Default

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

If you enter the sequence number of an existing map sequence, you enter port access-map mode. If you do not specify a sequence number, a number is automatically assigned. You can enter one match clause and one action clause per map sequence.

If you enter the **noportaccess-mapname** [*seq#*] command without entering a sequence number, the whole map is removed.

Once you enter port access-map mode, the following commands are available:

- **action** -- Specifies the packet action clause; see the **action** command section.
- **default** -- Sets a command to its defaults.
- **end** -- Exits from configuration mode.
- **exit** -- Exits from the port access-map configuration mode.
- **match** -- Specifies the match clause; see the **match** command section.
- **no** -- Negates a command or sets its defaults.

Examples

This example shows how to enter port access-map mode:

```
Router(config)# port access-map ted
Router(config-port-map)#
```

Related Commands

Command	Description
action	Sets the packet action clause.
match	Specifies the match clause by selecting one or more ACLs for a VLAN access-map sequence.

port-channel hash-distribution

To set the hash distribution algorithm method, use the port-channel hash-distribution command in global configuration mode. To return to the default settings, use the **no** or **default** form of this command.

port-channel hash-distribution {**adaptive** | **fixed**}
{**no** | **default**} **port-channel hash-distribution**

Syntax Description

adaptive	Specifies selective distribution of the bundle select register among the port-channel members.
fixed	Specifies fixed distribution of the bundle select register among the port-channel members.
default	Specifies the default setting.

Command Default

The hash distribution algorithm method is set to **fixed.**

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

The EtherChannel load distribution algorithm uses the bundle select register in the port ASIC to determine the port for each outgoing packet. When you use the **adaptive** algorithm, it does not require the bundle select register to be changed for existing member ports. When you use the **fixed** algorithm and you either add or delete a port from the EtherChannel, the switch updates the bundle select register for each port in the EtherChannel. This update causes a short outage on each port.

Note When you change the algorithm, the change is applied at the next member link event. Example events include link down, up, addition, deletion, no shutdown, and shutdown. When you enter the command to change the algorithm, the command console issues a warning that the command does not take effect until the next member link event.

Examples

The following example shows how to set the hash distribution algorithm method to adaptive:

```
Router(config)# port-channel hash-distribution adaptive
```

port-channel load-balance

To set the load distribution method among the ports in a bundle, use the **port-channelload-balance** command in global configuration mode. To reset the load distribution to the default settings, use the **no** form of this command.

port-channel load-balance *method* **module** *slot*
no port-channel load-balance

Syntax Description

method	Load distribution method; see the "Usage Guidelines" section for a list of valid values.
module	Specifies the module on which the load-distribution method is set. This keyword is supported only on DFC systems.
slot	Number of the slot in the module.

Command Default

The default**method** is **src-dst-ip**.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	This command was modified to support the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was modified. The following keywords were added: **dst-mixed-ip-port**,**src-dst-mixed-ip-port**,**src-mixed-ip-port**,and**excludevlan**. • These keywords are supported on systems that are in PFC3C or PFC3CXL mode (PFC3C or PFC3CXL with no DFC3A or DFC3B/BXL) only. • The **excludevlan**keyword is added only for IP-related load balance options.

Usage Guidelines

Valid *method* values are as follows:

- **dst-ip** --Loads distribution on the destination IP address. Option to exclude VLAN in the distribution is provided using the **excludevlan**keyword along with this method.
- **dst-mac** --Loads distribution on the destination MAC address.
- **dst-mixed-ip-port** --Loads distribution on the destination IP address and TCP or User Datagram Protocol (UDP) port. Option to exclude VLAN in the distribution is provided using the **excludevlan**keyword along with this method.
- **dst-port** --Loads distribution on the destination port.
- **src-dst-ip** --Loads distribution on the source transfer or XOR-destination IP address. Option to exclude VLAN in the distribution is provided using the **excludevlan**keyword along with this method.

- **src-dst-mac** --Loads distribution on the source XOR-destination MAC address.
- **src-dst-mixed-ip-port** --Loads distribution on the source XOR-destination IP address and the TCP or UDP port. Option to exclude VLAN in the distribution is provided using the **excludevlan**keyword along with this method.
- **src-dst-port** --Loads distribution on the source XOR-destination port.
- **src-ip** --Loads distribution on the source IP address. Option to exclude VLAN in the distribution is provided using the **excludevlan**keyword along with this method.
- **src-mac** --Loads distribution on the source MAC address.
- **src-mixed-ip-port** --Loads distribution on the source IP address and the TCP or UDP port. Option to exclude VLAN in the distribution is provided using the **excludevlan**keyword along with this method.
- **src-port** --Loads distribution on the source port.

The **port-channelload-balance***method***module***slot* command is supported on DFC systems only.

The **port-channelper-moduleload-balance** command allows you to enable or disable port-channel load-balancing on a per-module basis. You can enter the **port-channelload-balance***method***module***slot* command to specify the load-balancing method on a specific module after you have entered the **port-channelper-moduleload-balance**command.

The following keywords are supported on systems that are in PFC3C or PFC3CXL mode (PFC3C or PFC3CXL with no DFC3A or DFC3B/BXL) only:

- **dst-mixed-ip-port**
- **src-dst-mixed-ip-port**
- **src-mixed-ip-port**

Note If you change the load-balancing method, EtherChannel ports on DFC-equipped switching modules or an active supervisor engine in a dual supervisor engine configuration will flap.

Examples

The following example shows how to set the load-distribution method to **dst-ip**:

```
Router(config)#
port-channel load-balance dst-ip
```

The following example shows how to set the load-distribution method on a specific module:

```
Router(config)#
port-channel load-balance dst-ip module 2
```

The following example shows how to set the load-distribution method excluding the VLAN option:

```
Router(config)#
port-channel load-balance dst-ip exclude vlan
```

Related Commands

Command	Description
interface port-channel	Creates a port-channel virtual interface and enters interface configuration mode.
port-channel load-balance mpls	Sets the load distribution method among the ports in the bundle for MPLS packets.
show etherchannel	Displays the EtherChannel information for a channel.

port-channel load-balance (interface)

To configure a member link for load balancing, a default service instance weight, or weighted load balancing on port-channel member links, use the **port-channel load-balance** command in interface configuration mode. To cause the default weight to revert to 1 and to disable weighted load balancing, use the **no** form of this command.

port-channel load-balance {**link** *link-id* | **weighted** {**default weight** *weight* | **link** {**all***link-id*} | **rebalance** {**disable***weight*}}}
no port-channel load-balance {**link** *link-id* | **weighted** {**default weight** | **link** | **rebalance**}}

Syntax Description

link	Configures a member link for egress load balancing.
link-id	Integer from 1 to 16 that identifies the member link. • When used with the **weighted** keyword, the *link-id* is a comma-delimited list of member link IDs to use for weighted load balancing.
weighted	Configures weighted load balancing on the port channel.
default weight	Configures a default weight for a service instance.
weight	Integer from 1 to 10000 that is the weight value. The default is 1. • When used with the **rebalance** keyword, this value is the threshold weight used to trigger automatic rebalancing. The default is 4.
all	Configures load balancing across all active member links.
rebalance	Sets or disables the automatic rebalance threshold.
disable	Disables automatic rebalancing.

Command Default

Service instance weight and weighted load balancing are not configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.0(1)S	This command was introduced.

Usage Guidelines

When weighted load balancing enabled, the weight configured using this command is inherited by all service instances on the port channel that have not been specifically configured with a weight.

Configuring a default weight is optional; the default weight value is 1.

Use of the **weighted**and **link** keywords is required to enable weighted load balancing on a port channel. When the **all** keyword is configured, traffic is distributed across all active member links in the port channel. When one or more member links is specified, traffic is distributed across only those member links. To allow for out-of-order configuration, link IDs not yet assigned to member links may be specified. Issuing this command with the **weighted** and **link** keywords more than once under the same port-channel interface results in overwriting the command settings previously configured.

If this command is configured with a list of link IDs and the member link corresponding to one of those link IDs is later configured with a different ID, a warning is displayed on the console that notifies the user that the action will affect the current load-balancing activity.

When the **disable** keyword is configured, automatic rebalancing is not performed and the operator must manually invoke rebalancing by issuing the **port-channel load-balance weighted rebalance**command in privileged EXEC mode.

When the **disable** keyword is not configured, either the configured or a default weight is used to automatically rebalance service instances. Automatic rebalancing occurs when the average absolute deviation (AAD) of the current distribution exceeds the configured threshold and when the resulting AAD of the rebalanced distribution is less than the current AAD. If automatic rebalancing does not result in a lower AAD, the rebalancing is not done, even if the current AAD exceeds the threshold.

The AAD calculation is (1/*n*)*Sum(|w(*i*) - m|) for all *n* member links where:

n = number of member links

m = mean of member link weights (sum of all Ethernet service instance weights divided by *n*)

w (*i*) = sum of Ethernet service instance weights on member link *i*

Two conditions cause the **port-channel load-balance**command to fail:

- An invalid weight is configured.
- An invalid link ID is provided.

Examples

The following example shows how to configure port-channel load balancing for all port-channel member links:

```
Router(config)# interface port-channel1
Router(config-if)# port-channel load-balance weighted link all
```

port-channel load-balance mpls

To set the load-distribution method among the ports in the bundle for Multiprotocol Label Switching (MPLS) packets, use the **port-channel load-balance mpls**command in global configuration mode. To reset the load distribution to the default settings, use the **no** form of this command.

port-channel load-balance mpls {**label** | **label-ip**}
no port-channel load-balance mpls

Syntax Description

label	Specifies using the MPLS label to distribute packets; see the "Usage Guidelines" section for additional information.
label-ip	Specifies using the MPLS label or the IP address to distribute packets; see the "Usage Guidelines" section for additional information.

Command Default

label-ip

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

If you select **label**, these guidelines apply:

- With only one MPLS label, the last MPLS label is used.
- With two or more MPLS labels, the last two labels (up to the fifth label) are used.

If you select **label-ip**, these guidelines apply:

- With IPv4 and three or fewer labels, the source IP address XOR-destination IP address is used to distribute packets.
- With four or more labels, the last two labels (up to the fifth label) are used.
- With non-IPv4 packets, the distribution method is the same as the **label** method.

Examples

This example shows how to set the load-distribution method to **label-ip**:

```
Router(config)#
port-channel load-balance mpls label-ip
Router(config)#
```

Related Commands

Command	Description
interface port-channel	Creates a port-channel virtual interface and enters interface configuration mode.
show etherchannel	Displays the EtherChannel information for a channel.

port-channel load-balance weighted rebalance

To perform a rebalancing of all port-channel interfaces configured with weighted load balancing, use the **port-channel load-balance weighted rebalance** command in privileged EXEC mode.

port-channel load-balance weighted rebalance [**interface port-channel** *number*]

Syntax Description

interface	(Optional) Specifies a port channel enabled for weighted load balancing.
port-channel	(Optional) Specifies an Ethernet channel of interfaces.
number	(Optional) Integer from 1 to 564 that identifies the port-channel interface.

Command Default

Load rebalancing is not performed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)S	This command was introduced.

Usage Guidelines

If a port-channel interface is specified, only that interface is rebalanced; otherwise all port channels with weighted load balancing enabled are rebalanced.

This command may be used when automatic rebalancing is disabled via the **port-channel load-balance weighted rebalance disable** command or when a rebalancing of service instances is desired prior to reaching the automatic rebalance threshold.

If the specified interface is not a port channel enabled for weighted load balancing, the **port-channel load-balance weighted rebalance**command has no effect on load balancing on that interface.

Examples

The following example shows how to force a rebalancing of service instances, based on their assigned weights, for all port channels with weighted load balancing enabled:

```
Router# port-channel load-balance weighted rebalance
```

Related Commands

Command	Description
port-channel load-balance (interface)	Configures a member link for load balancing, a default service instance weight, or weighted load balancing on port-channel member links.

port-channel load-balancing vlan-manual

To apply the VLAN-manual load-balancing method globally to all Gigabit EtherChannel (GEC) interfaces, use the **port-channelload-balancingvlan-manual**command in global configuration mode. To reset to the default, use the **no** form of this command.

port-channel load-balancing vlan-manual
no port-channel load-balancing

Syntax Description

This command has no arguments or keywords.

Command Default

Flow-based load balancing is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. The default was changed from no load balancing is enabled to flow-based load balancing.

Usage Guidelines

The **port-channelload-balancingvlan-manual** command applies the VLAN-manual load-balancing method globally to all port channels on the router. If you do not use this command to explicitly set the global load-balancing method to VLAN-manual, the load-balancing method is set to flow-based.

The load-balancing method enabled on a port channel with the **load-balancing**command takes precedence over this command.

Load balancing uses the concept of buckets to map traffic flows to the member links of a port channel. The different traffic flows are mapped to the buckets and each bucket has one active member link associated with it. All flows that are mapped to a bucket use the member link associated with that bucket.

There are two methods of load balancing on a GEC interface:

- VLAN-manual--All packets forwarded over the same VLAN subinterface are considered part of the same flow and are mapped to the member link specified in the configuration.
- Flow-based--Traffic flows are mapped to different member links based on the packet header.

Examples

This example shows how to set the load-balancing method to VLAN-manual:

```
Router(config)# port-channel
load-balancing vlan-manual
```

Related Commands

Command	Description
interface port-channel	Creates a port-channel virtual interface.
load-balancing	Applies a load-balancing method to a GEC interface.

Command	Description
show interfaces port-channel etherchannel	Displays the load-balancing bucket distribution currently in use for a GEC interface.
show etherchannel load-balancing	Displays the load-balancing method applied to GEC interfaces.

port-channel load-defer

To configure the port load share deferral interval for all port channels, use the **port-channelload-defer** command in global configuration mode. To reset the port defer interval to the default setting, use the **no** form of this command.

port-channel load-defer *seconds*
no port-channel load-defer *seconds*

Syntax Description

seconds	Sets the time interval in seconds by which load sharing will be deferred on the switch. Valid range is from 1 to 1800 seconds. The default deferal interval is 120 seconds

Command Default

The port defer interval is 120 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(50)SY	This command was introduced. Added the *seconds* variable for use in Cisco IOS Release 12.2(50)SY.

Usage Guidelines

To reduce data loss following a stateful switchover (SSO), port load share deferral can be enabled by entering the **port-channelportload-defer** command on a port channel of a switch that is connected by a multichassis EtherChannel (MEC) to a virtual switching system (VSS). Port load share deferral temporarily prevents the switch from forwarding data traffic to MEC member ports on a failed chassis of the VSS while the VSS recovers from the SSO.

The load share deferral interval is determined by a single global timer configurable by the **port-channelload-defer** command. After an SSO switchover, a period of several seconds to several minutes can be required for the reinitialization of line cards and the reestablishment of forwarding tables, particularly multicast topologies.

The valid range of *seconds* is 1 to 1800 seconds; the default is 120 seconds.

Examples

This example shows how to set the global port deferral interval to 60 seconds:

```
Router(config)#
port-channel load-defer 60
Router(config)#
```

This example shows how to verify the configuration of the port deferral interval on a port channel:

```
Router# show etherchannel 50 port-channel

                Port-channels in the group:
                ----------------------
Port-channel: Po50    (Primary Aggregator)
------------
Age of the Port-channel   = 0d:00h:22m:20s
```

```
Logical slot/port   = 46/5          Number of ports = 3
HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   LACP
Fast-switchover     = disabled
Load share deferral = enabled   defer period = 60 sec
   time left = 57 sec
Router#
```

Related Commands

Command	Description
interface port-channel	Creates a port channel virtual interface and enters interface configuration mode.
port-channel port load-defer	Enables the port load share deferral feature on a port channel.
show etherchannel	Displays the EtherChannel information for a channel.

port-channel min-links

To specify that a minimum number of bundled ports in an EtherChannel is required before the channel can be active, use the **port-channelmin-links** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

port-channel min-links *min-num*
no port-channel min-links

Syntax Description

min-num	Minimum number of bundled ports in a channel that is required before the channel can be active; valid values are from 2 to 8.

Command Default

min-num is **1**

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXF	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported on LACP (802.3ad) ports only. More than one LACP secondary-port channel can belong to the same channel group. This command is applied to all port channels in the same group.

If fewer links than the specified number are available, the port-channel interface does not become active.

Use the **showrunning-config** command to verify the configuration.

Examples

This example shows how to specify that a minimum number of bundled ports in an EtherChannel is required before the channel can be active:

```
Router(config-if)#
port-channel min-links 3
Router(config-if)#
```

Related Commands

Command	Description
show running-config	Displays the status and configuration of the module or Layer 2 VLAN.

port-channel per-module load-balance

To enable load balance on a per-module basis among the ports in a bundle, use the port-channel per-module load-balance command in global configuration mode. To return to the default settings, use the **no** form of this command.

port-channel per-module load-balance
no port-channel per-module load-balance

Syntax Description

This command has no arguments or keywords.

Command Default

The load balance method is not enabled per module**.**

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **port-channelper-moduleload-balance** command allows you to enable or disable port-channel load balancing on a per-module basis. You can use the **port-channelload-balancemodule**command to specify the load balancing method on a specific module after you have entered the **port-channelper-moduleload-balance** command.

Examples

The following example shows how to enable load balancing on a per-module basis:

```
Router(config)# port-channel per-module load-balance
```

Related Commands

Command	Description
port-channel hash-distribution	Sets the hash distribution algorithm method among the ports in a bundle.
port-channel load-balance	Sets the load balance method among the ports in a bundle.

port-channel port load-defer

To enable the temporary deferral of port load sharing during the connection or reconnection of a port channel, use the **port-channelportload-defer** command in interface configuration mode. To disable the deferral of port load sharing on a port channel, use the **no** form of this command.

port-channel port load-defer
no port-channel port load-defer

Syntax Description

This command has no keywords or arguments.

Command Default

The port load share deferral feature is not enabled on a port channel .

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(50)SY	This command was introduced.

Usage Guidelines

To reduce data loss following a stateful switchover (SSO), a port load share deferral can be enabled on a port channel of a switch that is connected by a multichassis EtherChannel (MEC) to a virtual switching system (VSS). The load share deferral interval prevents the switch from forwarding data traffic to MEC member ports on a failed chassis of the VSS while the VSS recovers from the SSO.

When load share deferral is enabled on a port channel, the assignment of a member port's load share is delayed for a period that is configurable globally by the **port-channelload-defer** command. During the deferral period, the load share of a deferred member port is set to 0. In this state, the deferred port is capable of receiving data and control traffic, and of sending control traffic, but the port is prevented from sending data traffic over the MEC to the VSS. Upon expiration of the global deferral timer, the deferred member port exits the deferral state and the port assumes its normal configured load share.

Load share deferral is applied only if at least one other member port of the port channel is currently active with a nonzero load share. If a port enabled for load share deferral is the first member bringing up the EtherChannel, the deferral feature does not apply and the port will forward traffic immediately.

The load share deferral interval is determined by a single global timer configurable from 1 to 1800 seconds by the **port-channelload-defer** command. The default interval is 120 seconds. After an SSO switchover, a period of several seconds to several minutes can be required for the reinitialization of line cards and the reestablishment of forwarding tables, particularly multicast topologies.

Examples

This example shows how to enable the load share deferral feature on port channel 50 of a switch that is an MEC peer to a VSS:

```
Router(config)#
interface port-channel 50
Router(config-if)#
port-channel port load-defer

This will enable the load share deferral feature on this port-channel.
```

```
The port-channel should connect to a Virtual Switch (VSS).
Do you wish to proceed? [yes/no]:
yes
Router(config-if)#
```

This example shows how to verify the state of the port deferral feature on a port channel:

```
Router# show etherchannel 50 port-channel

                Port-channels in the group:
                ----------------------
Port-channel: Po50    (Primary Aggregator)
------------
Age of the Port-channel   = 0d:00h:22m:20s
Logical slot/port   = 46/5          Number of ports = 3
HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   LACP
Fast-switchover     = disabled
Load share deferral = enabled   defer period = 120 sec   time left = 57 sec
Router#
```

Related Commands

Command	Description
interface port-channel	Creates a port channel virtual interface and enters interface configuration mode.
port-channel load-defer	Configures the global port load share deferral time interval for port channels.
show etherchannel	Displays the EtherChannel information for a channel.

port-channel standalone-disable

To disable the EtherChannel standalone option in a port channel, use the **port-channel standalone-disable** command in interface configuration mode. To enable this option, use the **no** form of this command.

port-channel standalone-disable
no port-channel standalone-disable

Syntax Description

This command has no arguments or keywords.

Command Default

The EtherChannel standalone option is enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI3	This command was introduced.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.

Usage Guidelines

The **port-channel standalone-disable** command is supported on the Catalyst 6000 series switches. This command can be used only when the port-channel protocol type is Link Aggregation Control Protocol (LACP). This command enables you to change the current behavior when a physical port cannot bundle an LACP EtherChannel.

Examples

The following example shows how to disable the EtherChannel standalone option in a port channel:

```
Device(config-if)# port-channel standalone-disable
```

Related Commands

Command	Description
show etherchannel	Displays the EtherChannel information for a channel.

pos ais-shut

To send the line alarm indication signal (LAIS) when the Packet-over-SONET (POS) interface is placed in any administrative shutdown state, use the pos ais-shut command in interface configuration mode.

pos ais-shut

Syntax Description

This command has no arguments or keywords.

Command Default

No LAIS is sent.

Command Modes

Interface configuration

Command History

Release	Modification
11.1CC	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

In Automatic Protection Switching (APS) environments, LAIS can be used to force a protection switch. This command forces an APS switch when the interface is placed in the administrative shutdown state.

For more information on APS, refer to the “Configuring Serial Interfaces” chapter in the Cisco IOS Interface and Hardware Component Configuration Guide.

This command does not have a **no** form.

Examples

The following example forces the alarm indication on POS OC-3 interface 0 in slot 3:

```
Router(config)# interface pos 3/0
Router(config-if)# shutdown
Router(config-if)# pos ais-shut
```

pos delay triggers

To enable a POS alarm trigger delay, or to enable path level alarms as triggers to bring the POS line card protocol to down, use the pos delay triggers command in POS interface configuration mode. To disable POS alarm trigger delays, use the **no** form of this command.

pos delay triggers [{**line** *ms* | **path** *ms*}]
no pos delay triggers [{**line** *ms* | **path** *ms*}]

Syntax Description

line	Specifies the delay for SONET line level triggers. The following alarms are considered line level triggers: section loss of signal, section loss of frame, line alarm indication signal. SONET line level triggers bring the line protocol down by default
path	Specifies that SONET path level alarms should trigger the line protocol to go down.
ms	Specifies the time, in milliseconds, that POS trigger should wait before setting the line protocol to down. If no *ms* value is entered, the default value of 100 ms is used.

Command Default

POS line level alarm triggers are enabled by default. If a POS line level alarm trigger occurs and no configuration changes have been made using the**posdelaytriggersline***ms*command, the line protocol is set to down immediately with no delay.

POS path level alarm triggers are disabled by default. A path level alarm will not set the line protocol to down unless the **posdelaytriggerspath** command has been entered.

If no *ms* value is entered but **posdelaytriggersline** command is configured, the default *ms* value for line level triggers is 100 ms.

If no *ms* value is entered and **posdelaytriggerspath** is enabled, the default *ms* value is set at 100 ms for path level triggers.

Command Modes

POS interface configuration

Command History

Release	Modification
12.1(12c)EX1	This command was introduced for Cisco 7304 routers.
12.2(18)S	This command was introduced on Cisco 7304 routers running Cisco IOS Release 12.2S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4	This command was integrated into Cisco IOS Release 12.4 Mainline. This command supports Cisco 7200 Series, Cisco 7304 Series, and Cisco 7600 Series routers.
12.4(24)T	This command was integrated into a release earlier than Cisco IOS Release 12.4(24)T. This command supports Cisco 7200 Series, Cisco 7304 Series, and Cisco 7600 Series routers.

Usage Guidelines

A trigger is an alarm that, when asserted, causes the line protocol to go down.

When one or more triggers are asserted, the line protocol of the interface goes down. The POS Alarm Trigger Delay feature provides the option to delay triggering of the line protocol of the interface from going down when an alarm triggers the line protocol to go down. For instance, if you configure the POS alarm delay for 150 ms, the line protocol will not go down for 150 ms after receiving the trigger. If the trigger alarm stays up for more than 150 ms, the link is brought down as it is now. If the trigger alarm clears before 150 ms, the line protocol is not brought down.

By default, the following line and section alarms are triggers for the line protocol to go down:

- Section loss of signal
- Section loss of frame
- Line alarm indication signal

For line and section alarm triggers, the line protocol of the POS card is brought down immediately if a trigger is received and no POS alarm trigger delay is specified. The delay can be set anywhere from 50 to 10000 ms. If POS alarm triggering is configured but no *ms* value is entered, the POS alarm trigger delay is 100 ms.

The following path alarms are not triggers by default. These path alarms, however, can be configured as triggers:

- Path alarm indication signal
- Path remote defect indication

The POS Alarm Trigger Delay feature can be used to configure these alarms as triggers, as well as to configure the exact POS alarm trigger delay for these triggers. The default delay values for these triggers, if no value is specified, is also 100 ms.

Examples

In the following configuration example, the POS line card will wait 50 ms after receiving a line level trigger before setting the line protocol to down. If the alarm that began the line level trigger clears during that 50 ms, the line protocol will remain up. If the alarm that began the line trigger remains after that 50 ms, the line protocol will go down.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface pos 1/0
Router(config-if)# pos delay triggers line 50
```

In the following configuration example, the POS line card will wait 110 ms after receiving a path trigger before setting the line protocol to down. If the alarm that began the path trigger clears during that 110 ms, the line protocol will remain up. If the alarm that began the path trigger remains after 110 ms, the line protocol will go down.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface pos 1/0
Router(config-if)# pos delay triggers path 110
```

In the following example, the **showcontrollerspos***slot*/*interface-number***detail** command is used to verify the POS alarm trigger delay. In this particular example, the delay is 100 ms (italicized for emphasis below) for both line level triggers and path level triggers.

```
Router# show controllers pos 4/0 detail
```

POS4/0

SECTION

LOF = 0 LOS = 0 BIP(B1) = 22

LINE

AIS = 0 RDI = 0 FEBE = 21 BIP(B2) = 38

PATH

AIS = 0 RDI = 1 FEBE = 25 BIP(B3) = 31

PLM = 0 UNEQ = 0 TIM = 0 TIU = 0

LOP = 0 NEWPTR = 4 PSE = 2 NSE = 3

Active Defects:None

Active Alarms: None

Alarm reporting enabled for:SF SLOS SLOF B1-TCA B2-TCA PLOP B3-TCA

Line triggers delayed 100 ms

```
Path triggers delayed 100 ms
...
```

Related Commands

Command	Description
show controllers pos *slot* / *interface-number* **detail**	Shows the content of POS controllers, including the amount of delay for line triggers.

pos flag

To set the SONET overhead bytes in the frame header to meet a specific standards requirement or to ensure interoperability with the equipment of another vendor, use the **posflag**command in interface configuration mode. To remove the setting of the SONET overhead bytes, use the **no** form of this command.

pos flag commandpos flag {**c2** | **j0** | **s1s0**} *value*
no pos flag {**c2** | **j0** | **s1s0**} *value*

Syntax Description

c2 *value*	Path signal identifier used to identify the payload content type. The default value is 0xCF.
j0 *value*	Section trace byte (formerly the C1 byte). For interoperability with Synchronous Digital Hierarchy (SDH) equipment in Japan, use the value 0x1. The byte value can be 0 to 255.
sls0 *value*	S1 and S0 bits (bits 5 and 6 of the H1 #1 payload pointer byte). Use the following values to tell the SONET transmission equipment the SS bit: • For OC-3c, use 0 (this is the default). • For AU-4 container in SDH, use 2. The S1 and S0 bits can be 0 to 3. Values 1 and 3 are undefined. The default value is 0.

Command Default

The default **c2** value is 0xCF. The default **sls0** value is 0.

Command Modes

Interface configuration

Command History

Release	Modification
11.2 GS	This command was introduced to support the Cisco 12000 series Internet routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the following values to tell the SONET transmission equipment the payload type:

- For PPP, or High-Level Data Link Control (HDLC) when required, use 0xCF (this is the default).
- For ATM, use 0x13.
- For other equipment, use any nonzero value.
- The byte value can be 0 to 255.

Examples

The following example sets the path signal identifier used to identify the payload content type to ATM on the **pos** interface in slot 9:

```
Router(config)# interface pos 9/0
```

```
Router(config-if)# pos flag c2 0x13
Router(config-if)# end
```

pos flag s1-byte rx-communicate

To direct the router to switch to internal clocking when it receives an S1 SONET overhead byte with a value of 0xF, use the pos flag s1-byte rx-communicate command in interface configuration mode. To disable this capability, use the **no** form of this command.

pos flag s1-byte rx-communicate
no pos flag s1-byte rx-communicate

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced on the Cisco 10000 series router.

Usage Guidelines

The pos flag s1-byte rx-communicate command directs the router to switch the clock source to internal when it receives an S1 SONET overhead byte with a value of 0xF. When the S1 SONET overhead byte changes from 0xF to any other value, the clock source reverts back to the clock source specified in the user configuration.

The S1 SONET overhead byte is ignored by the receiving router unless the pos flag s1-byte rx-communicate command is issued.

Examples

The following example directs the router to switch to internal clocking when it receives an S1 SONET overhead byte with a value of 0xF:

```
pos flag s1-byte rx-communicate
```

Related Commands

Command	Description
pos flag	Assigns values for specific elements of the frame header. This command is typically used to meet a standards requirement or to ensure interoperability with another vendor's equipment.
pos flag s1-byte tx	Controls the transmission of the S1 SONET overhead byte.

pos flag s1-byte tx

To control the transmission of the S1 SONET overhead byte, use the pos flag s1-byte tx command in interface configuration mode.

pos flag s1-byte tx *value*

Syntax Description

value	Set the S1 SONET overhead byte to a value in the range of 0x0 to 0xF.

Command Default

The default is 0x0.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced on the Cisco 10000 series router.

Usage Guidelines

In most situations, the default value for the S1 SONET overhead byte does not need to be changed. Refer to the SONET standards for information about the possible values for the S1 SONET overhead byte and the definition of each value.

Examples

The following example sets the S1 SONET overhead byte to 0xF:

```
pos flag s1-byte tx 0xF
```

Related Commands

Command	Description
pos flag	Assigns values for specific elements of the frame header. This command is typically used to meet a standards requirement or to ensure interoperability with another vendor's equipment.
pos flag s1-byte rx-communicate	Directs the router to switch to internal clocking when it receives an S1 SONET overhead byte with a value of 0xF.

pos framing

To specify the framing used on the POS (Packet-over-SONET) interface, use the **posframing** command in interface configuration mode. To return to the default SONET STS-3c framing mode, use the **no** form of this command.

pos framing commandpos framing {**sdh** | **sonet**}
no pos framing

Syntax Description

sdh	Selects SDH STM-1 framing. This framing mode is typically used in Europe.
sonet	Selects SONET STS-3c framing. This is the default.

Command Default

SONET STS-3c framing

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
11.3	This command was modified to change the **posiframing-sdh** command to **posframing-sdh**.
11.2GS	The command syntax was changed from **posframing-sdh** to **posframing**. The **sonet** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example configures the interface for SDH STM-1 framing:

```
Router(config)# interface pos 3/0
Router(config-if)# pos framing sdh
Router(config-if)# no shutdown
```

Related Commands

Command	Description
clock source (interface)	Controls the clock used by a G.703-E1 interface.
interface	Configures an interface type, and enters interface configuration mode.

pos report

To permit selected SONET alarms to be logged to the console for a POS (Packet-over-SONET) interface, use the **posreport**command in interface configuration mode. To disable logging of select SONET alarms, use the **no** form of this command.

pos report commandpos report {**b1-tca** | **b2-tca** | **b3-tca** | **lais** | **lrdi** | **pais** | **plop** | **prdi** | **rdool** | **sd-ber** | **sf-ber** | **slof** | **slos**}
no pos report {**b1-tca** | **b2-tca** | **b3-tca** | **lais** | **lrdi** | **pais** | **plop** | **prdi** | **rdool** | **sd-ber** | **sf-ber** | **slof** | **slos**}

Syntax Description

b1-tca	Reports B1 bit-error rate (BER) threshold crossing alarm (TCA) errors.
b2-tca	Reports B2 BER crossing TCA errors.
b3-tca	Reports B3 BER crossing TCA errors.
lais	Reports line alarm indication signal errors.
lrdi	Reports line remote defect indication errors.
pais	Reports path alarm indication signal errors.
plop	Reports path loss of pointer errors.
prdi	Reports path remote defect indication errors.
rdool	Reports receive data out of lock errors.
sd-ber	Reports signal degradation BER errors.
sf-ber	Reports signal failure BER errors.
slof	Reports section loss of frame errors.
slos	Reports section los of signal errors.

Command Default

The following alarms are reported by default:

- **b1-tca**
- **b2-tca**
- **b3-tca**
- **plop**
- **sf-ber**
- **slof**
- **slos**

Command Modes

Interface configuration

Command History

Release	Modification
11.1CC	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Reporting an alarm means that the alarm can be logged to the console. Just because an alarm is permitted to be logged does not guarantee that it is logged. SONET alarm hierarchy rules dictate that only the most severe alarm of an alarm group is reported. Whether an alarm is reported or not, you can view the current state of a defect by checking the "Active Defects" line from the **showcontrollerspos**command output. A defect is a problem indication that is a candidate for an alarm.

For B1, the bit interleaved parity error report is calculated by comparing the BIP-8 code with the BIP-8 code extracted from the B1 byte of the following frame. Differences indicate that section level bit errors have occurred.

For B2, the bit interleaved parity error report is calculated by comparing the BIP-8/24 code with the BIP-8 code extracted from the B2 byte of the following frame. Differences indicate that line level bit errors have occurred.

For B3, the bit interleaved parity error report is calculated by comparing the BIP-8 code with the BIP-8 code extracted from the B3 byte of the following frame. Differences indicate that path level bit errors have occurred.

PAIS is sent by line terminating equipment (LTE) to alert the downstream path terminating equipment (PTE) that it has detected a defect on its incoming line signal.

PLOP is reported as a result of an invalid pointer (H1, H2) or an excess number of new data flag (NDF) enabled indications.

SLOF is detected when a severely error framing (SEF) defect on the incoming SONET signal persists for 3 milliseconds.

SLOS is detected when an all-zeros pattern on the incoming SONET signal lasts 19 plus or minus 3 microseconds or longer. This defect might also be reported if the received signal level drops below the specified threshold.

To determine the alarms that are reported on the interface, use the **showcontrollerspos**command.

Examples

The following example enables reporting of SD-BER and LAIS alarms on the interface:

```
Router(config)# interface pos 3/0/0
Router(config-if)# pos report sd-ber
Router(config-if)# pos report lais
Router(config-if)# end
```

Related Commands

Command	Description
interface	Configures an interface type, and enters interface configuration mode.
show controllers pos	Displays information about the POS controllers.

pos scramble-atm

To enable SONET payload scrambling on a POS (Packet-over-SONET) interface, use the **posscramble-atm**command in interface configuration mode. To disable scrambling, use the **no** form of this command.

pos scramble-atm commandpos scramble-atm
no pos scramble-atm

Syntax Description

This command has no arguments or keywords.

Command Default

Scrambling is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.1CA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

SONET payload scrambling applies a self-synchronous scrambler (x43+1) to the Synchronous Payload Envelope (SPE) of the interface to ensure sufficient bit transition density. Both ends of the connection must use the same scrambling algorithm. When enabling POS scrambling on a VIP2 POSIP on the Cisco 7500 series router that has a hardware revision of 1.5 or higher, you can specify CRC 16 only (that is, CRC 32 is currently not supported).

To determine the hardware revision of the POSIP, use the **showdiag** command.

To determine whether scrambling is enabled on the interface, use the **showinterfacepos** command or the **showrunning-config** command.

Note SONET payload scrambling is enabled with the **posscramble-atm** command. SONET payload scrambling applies a self-synchronous scrambler (x43+1) to the Synchronous Payload Envelope (SPE) of the interface to ensure sufficient bit transition density. Both sides of the connection must be configured using the **posscramble-atm** command. Currently, when connecting to a Cisco 7500 series router and using the **posscramble-atm** command, you must specify the **crc16** command rather than the **crc32** command.

Examples

The following example enables scrambling on the interface:

```
Router(config)# interface pos 3/0
Router(config-if)# pos scramble-atm
Router(config-if)# no shutdown
Router(config-if)# end
```

Related Commands

Command	Description
crc	Sets the length of the CRC on an FSIP or HIP of the Cisco 7500 series routers or on a 4-port serial adapter of the Cisco 7200 series routers.
interface	Configures an interface type, and enters interface configuration mode.
show diag	Displays hardware information for the router.
show interfaces pos	Displays information about the Packet OC-3 interface in Cisco 7500 series routers.

pos threshold

To set the bit-error rate (BER) threshold values of the specified alarms for a POS (Packet-Over-SONET) interface, use the **posthreshold**command in interface configuration mode. To return to the default setting, use the **no** form of this command.

pos threshold {**b1-tca** | **b2-tca** | **b3-tca** | **sd-ber** | **sf-ber**} *rate*
no pos threshold {**b1-tca** | **b2-tca** | **b3-tca** | **sd-ber** | **sf-ber**} *rate*

Syntax Description

b1-tca	B1 BER threshold crossing alarm. The default rate is 6.
b2-tca	B2 BER threshold crossing alarm. The default rate is 6.
b3-tca	B3 BER threshold crossing alarm. The default rate is 6.
sd-ber	Signal degrade BER threshold. The default rate is 6.
sf-ber	Signal failure BER threshold. The default rate is 3 (10e-3).
rate	Bit-error rate from 3 to 9 (10-n).

Command Default

The default rate is 6 for **b1-tca**, **b2-tca**, **b3-tca**, and **sd-ber**. The default rateis 3 (10e-3) for **sf-ber**.

Command Modes

Interface configuration

Command History

Release	Modification
11.1CC	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

For B1, the bit interleaved parity error report is calculated by comparing the BIP-8 code with the BIP-8 code extracted from the B1 byte of the following frame. Differences indicate that section level bit errors have occurred.

For B2, the bit interleaved parity error report is calculated by comparing the BIP-8/24 code with the BIP-8 code extracted from the B2 byte of the following frame. Differences indicate that line level bit errors have occurred.

For B3, the bit interleaved parity error report is calculated by comparing the BIP-8 code with the BIP-8 code extracted from the B3 byte of the following frame. Differences indicate that path level bit errors have occurred.

SF-BER and SD-BER are sourced from B2 BIP-8 error counts (as is B2-TCA). However, SF-BER and SD-BER feed into the automatic protection switching (APS) machine and can lead to a protection switch (if APS is configured).

B1-TCA, B2-TCA, and B3-TCA do nothing more than print a log message to the console (if reports for them are enabled).

To determine the BER thresholds configured on the interface, use the **showcontrollerspos**command.

Examples

The following example configures thresholds on the interface:

```
Router(config)# interface pos 3/0/0
Router(config-if)# pos threshold sd-ber 8
Router(config-if)# pos threshold sf-ber 4
Router(config-if)# pos threshold b1-tca 4
Router(config-if)# end
```

Related Commands

Command	Description
interface	Configures an interface type, and enters interface configuration mode.
pos report	Permits selected SONET alarms to be logged to the console for a POS interface.
show controllers pos	Displays information about the POS controllers.

power inline

To determine how inline power is applied to the device on the specified switch port, use the **powerinline** command in interface configuration mode. To return the setting to its default, use the **no** form of this command.

power inline {**auto** [**max** *max-milliwatts*] | **never** | **police** | **static** [**max** *max-milliwatts*]}
no power inline [**police**]

Cisco Integrated Services Routers Generation 2 (ISR G2) with Cisco Gigabit EtherSwitch enhanced high-speed WAN interface cards (EHWICs)
power inline {**auto** | **never** | **port max** *max-milliwatts*}
no power inline {**auto** | **never** | **port max** *max-milliwatts*}

Cisco 4451-X Integrated Services Router
power inline
auto | [**max** *max-milliwatts*] | **never** | **redundant**
no power inline
auto | [**max** *max-milliwatts*] | **never** | **redundant**

Syntax Description

auto	Turns on the device discovery protocol and applies power to the device, if found.
max *max-milliwatts*	(Optional) Specifies the maximum amount of power, in milliwatts, that a device connected to a port can consume. Range: 4000 to 16800. Default: 15400.
never	Turns off the device discovery protocol and stops supplying power to the device.
police	Turns on inline power policing; optional if entering the **no** form of the command. Default is disabled.
static	Allocates power from the system power pool to a port.
port max *max-milliwatts*	Specifies the maximum power allocated to the port. The maximum power can be set between 4,000 to 20,000 milliwatts.
redundant	Puts the inline power supply in redundant mode (default mode). (For boost mode, use the no form of the command; for example, **no power inline redundant**.)

Command Default

Power is applied when a telephone is detected on the port (**auto**).*max-milliwatts* is 15400 milliwatts. Inline power policing is disabled.

Power is applied when a telephone is detected on the port (auto). The maximum power limit is 20000 milliwatts. Inline power policing is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(5)XU	This command was introduced.
12.2(2)XT	This command was integrated to support switchport creation on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T to support switchport creation .
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17b)SXA	This command was changed to include the **static** and **max***max-milliwatts* keywords and arguments.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(33)SXH	This command was changed to include the **police** keyword .
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH2	This command was changed to increase the *max-watts* maximum to 16800 milliwatts for the WS-F6K-48-AF and the WS-F6K-GE48-AF modules. The default setting remains 15400 milliwatts. See the "Usage Guidelines" section for additional information.
15.1(2)T	This command was modified. The **portmax**keyword and *max-milliwatts* argument were added.
Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S.

Usage Guidelines

The **police**keyword appears if you have a WS-F6K-48-AF or other inline power daughter card that supports power monitoring and inline power policing.

Inline power is supported only on switch ports that are connected to an IP phone. Before you enable inline power on a switch port, you must enter the **switchport** command.

The following information applies to WS-F6K-48-AF and WS-F6K-GE48-AF inline power cards:

- In Cisco IOS Release 12.2(33)SXH2 and later releases, the configurable range of maximum power using the max keyword is 4000 to 16800 milliwatts. For earlier releases, the configurable range for maximum power is 4000 to 15400 milliwatts. For all releases, if no maximum power level is configured, the default maximum power is 15400 milliwatts.

Note To support a large number of inline-powered ports using power levels above 15400 milliwatts on an inline power card, we recommend using the static keyword so that the power budget is deterministic.

- In Cisco IOS Release 12.2(33)SXH2 and later releases, when you enter the auto keyword and CDP is enabled on the port, an inline-powered device that supports CDP can negotiate a power level up to 16800 milliwatts unless a lower maximum power level is configured. For earlier releases, the inline-powered device can negotiate a power level up to 15400 milliwatts or the configured maximum power level, if it is configured lower than 15400 milliwatts.

Cisco ISR G2 with Cisco Gigabit EHWICs

- The **portmax**keyword and *max-milliwatts* argument are available only on the Firebee cards with Power-over-Ethernet (PoE).

Examples

The following example shows how to set the inline power to the off mode on a switch port:

```
Router(config)# interface fastethernet5/1
Router(config-if)# switchport
Router(config-if)# power inline never
```

The following example shows how to allocate power from the system power pool to a switch port:

```
Router(config)# interface fastethernet5/1
Router(config-if)# switchport
Router(config-if)# power inline static max 15000
```

The following example shows how to turn on inline power policing to a switch port:

```
Router(config)# interface gigabitethernet6/3
Router(config-if)# switchport
Router(config-if)# power inline police
```

Cisco ISR G2 with Cisco Gigabit EtherSwitch EHWICs

The following example shows how to turn on inline power to a switch port:

```
Router(config)# interface gigabitethernet
0/1/3
Router(config-if)#
power inline
auto{!-condition!}
```

The following example shows how to set maximum inline power to a switch port:

```
Router(config)# interface
 gigabitethernet
0/1/3
```

The following example shows how to disable inline power to the switch port:

```
Router(config)# interface
 gigabitethernet

0/1/3
Router(config-if)# power inline
 never{!-condition!}
```

Cisco 4451-X Integrated Service Router

The following example shows auto option for power inline command configured on the front panel Gigabit Ethernet port.

```
Router(config)# interface gigabitEthernet 0/0/0
Router(config-if)# power inline auto
```

In this example, an attempt is made to configure the inline power to be in boost mode by using the **no** form of the **power inline redundant** command. The inline power mode is not changed to boost mode because that requires a total power available in redundant mode of 1000W.

```
Router# show power
Main PSU :
Configured Mode : Boost
Current runtime state same : Yes
Total power available : 2000 Watts
POE Module :
Configured Mode : Boost
Current runtime state same : Yes
Total power available : 1000 Watts
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# no power inline redundant
*Jan 31 03:42:40.947: %PLATFORM_POWER-6-MODEMISMATCH: Inline power not in Boost mode
Router(config)# exit
*Jan 31 03:36:13.111: %SYS-5-CONFIG_I: Configured from console by console
Router# show power
Main PSU :
Configured Mode : Boost
Current runtime state same : Yes
Total power available : 1450 Watts
POE Module :
Configured Mode : Boost
Current runtime state same : No
Total power available : 500 Watts
```

In this example, power for the main power supply is configured to be in boost mode by using the **no** form of the **power main redundant** command. This sets the power for the main power supply in boost mode to be 1450 W and the inline power in redundant mode as 500W.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# no power main redundant
Router(config)#
*Jan 31 03:35:22.284: %PLATFORM_POWER-6-MODEMATCH: Inline power is in Redundant mode
Router(config)#
Router(config)# exit
Router#
*Jan 31 03:36:13.111: %SYS-5-CONFIG_I: Configured from console by console
Router# show power
Main PSU :
Configured Mode : Boost
Current runtime state same : Yes
Total power available : 1450 Watts
POE Module :
Configured Mode : Redundant
Current runtime state same : Yes
Total power available : 500 Watts
Router#
```

Related Commands

Command	Description
show power inline	Displays the power status for the specified port or for all ports.
switchport priority extend	Determines how the telephone connected to the specified port handles priority traffic received on its incoming port.
switchport voice vlan	Configures the voice VLAN on the port.

power enable

To turn on power for the modules, use the **power enable**command in global configuration mode. To power down a module, use the **no** form of this command.

power enable module *slot*
no power enable module *slot*

Syntax Description

module *slot*	Specifies a module slot number; see the "Usage Guidelines" section for valid values.

Command Default

Enabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXD	This command was changed to allow you to disable power to empty slots.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

When you enter the **no power enable module** *slot* command to power down a module, the module's configuration is not saved.

When you enter the **no power enable module** *slot* command to power down an empty slot, the configuration is saved.

The *slot* argument designates the module number. Valid values for *slot*depend on the chassis that is used. For example, if you have a 13-slot chassis, valid values for the module number are from 1 to 13.

Examples

This example shows how to turn on the power for a module that was previously powered down:

```
Router(config)#
power enable module 5
Router(config)#
```

This example shows how to power down a module:

```
Router(config)#
no power enable module 5
Router(config)#
```

Related Commands

Command	Description
show power	Displays information about the power status.

power inline

To determine how inline power is applied to the device on the specified switch port, use the **powerinline** command in interface configuration mode. To return the setting to its default, use the **no** form of this command.

power inline {**auto** [**max** *max-milliwatts*] | **never** | **police** | **static** [**max** *max-milliwatts*]}
no power inline [**police**]

Cisco Integrated Services Routers Generation 2 (ISR G2) with Cisco Gigabit EtherSwitch enhanced high-speed WAN interface cards (EHWICs)
power inline {**auto** | **never** | **port max** *max-milliwatts*}
no power inline {**auto** | **never** | **port max** *max-milliwatts*}

Cisco 4451-X Integrated Services Router
power inline
auto | [**max** *max-milliwatts*] | **never** | **redundant**
no power inline
auto | [**max** *max-milliwatts*] | **never** | **redundant**

Syntax Description

auto	Turns on the device discovery protocol and applies power to the device, if found.
max *max-milliwatts*	(Optional) Specifies the maximum amount of power, in milliwatts, that a device connected to a port can consume. Range: 4000 to 16800. Default: 15400.
never	Turns off the device discovery protocol and stops supplying power to the device.
police	Turns on inline power policing; optional if entering the **no** form of the command. Default is disabled.
static	Allocates power from the system power pool to a port.
port max *max-milliwatts*	Specifies the maximum power allocated to the port. The maximum power can be set between 4,000 to 20,000 milliwatts.
redundant	Puts the inline power supply in redundant mode (default mode). (For boost mode, use the no form of the command; for example, **no power inline redundant**.)

Command Default

Power is applied when a telephone is detected on the port (**auto**).*max-milliwatts* is 15400 milliwatts. Inline power policing is disabled.

Power is applied when a telephone is detected on the port (auto). The maximum power limit is 20000 milliwatts. Inline power policing is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(5)XU	This command was introduced.
12.2(2)XT	This command was integrated to support switchport creation on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T to support switchport creation .
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17b)SXA	This command was changed to include the **static** and **max***max-milliwatts* keywords and arguments.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(33)SXH	This command was changed to include the **police** keyword .
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH2	This command was changed to increase the *max-watts* maximum to 16800 milliwatts for the WS-F6K-48-AF and the WS-F6K-GE48-AF modules. The default setting remains 15400 milliwatts. See the "Usage Guidelines" section for additional information.
15.1(2)T	This command was modified. The **portmax**keyword and *max-milliwatts* argument were added.
Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S.

Usage Guidelines

The **police**keyword appears if you have a WS-F6K-48-AF or other inline power daughter card that supports power monitoring and inline power policing.

Inline power is supported only on switch ports that are connected to an IP phone. Before you enable inline power on a switch port, you must enter the **switchport** command.

The following information applies to WS-F6K-48-AF and WS-F6K-GE48-AF inline power cards:

- In Cisco IOS Release 12.2(33)SXH2 and later releases, the configurable range of maximum power using the max keyword is 4000 to 16800 milliwatts. For earlier releases, the configurable range for maximum power is 4000 to 15400 milliwatts. For all releases, if no maximum power level is configured, the default maximum power is 15400 milliwatts.

Note To support a large number of inline-powered ports using power levels above 15400 milliwatts on an inline power card, we recommend using the static keyword so that the power budget is deterministic.

- In Cisco IOS Release 12.2(33)SXH2 and later releases, when you enter the auto keyword and CDP is enabled on the port, an inline-powered device that supports CDP can negotiate a power level up to 16800 milliwatts unless a lower maximum power level is configured. For earlier releases, the inline-powered device can negotiate a power level up to 15400 milliwatts or the configured maximum power level, if it is configured lower than 15400 milliwatts.

Cisco ISR G2 with Cisco Gigabit EHWICs

- The **portmax**keyword and *max-milliwatts* argument are available only on the Firebee cards with Power-over-Ethernet (PoE).

Examples

The following example shows how to set the inline power to the off mode on a switch port:

```
Router(config)# interface fastethernet5/1
Router(config-if)# switchport
Router(config-if)# power inline never
```

The following example shows how to allocate power from the system power pool to a switch port:

```
Router(config)# interface fastethernet5/1
Router(config-if)# switchport
Router(config-if)# power inline static max 15000
```

The following example shows how to turn on inline power policing to a switch port:

```
Router(config)# interface gigabitethernet6/3
Router(config-if)# switchport
Router(config-if)# power inline police
```

Cisco ISR G2 with Cisco Gigabit EtherSwitch EHWICs

The following example shows how to turn on inline power to a switch port:

```
Router(config)# interface gigabitethernet
0/1/3
Router(config-if)#
power inline
auto{!-condition!}
```

The following example shows how to set maximum inline power to a switch port:

```
Router(config)# interface
 gigabitethernet
0/1/3
```

The following example shows how to disable inline power to the switch port:

```
Router(config)# interface
 gigabitethernet

0/1/3
Router(config-if)# power inline
 never{!-condition!}
```

Cisco 4451-X Integrated Service Router

The following example shows auto option for power inline command configured on the front panel Gigabit Ethernet port.

```
Router(config)# interface gigabitEthernet 0/0/0
Router(config-if)# power inline auto
```

In this example, an attempt is made to configure the inline power to be in boost mode by using the **no** form of the **power inline redundant** command. The inline power mode is not changed to boost mode because that requires a total power available in redundant mode of 1000W.

```
Router# show power
Main PSU :
Configured Mode : Boost
Current runtime state same : Yes
Total power available : 2000 Watts
POE Module :
Configured Mode : Boost
Current runtime state same : Yes
Total power available : 1000 Watts
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# no power inline redundant
*Jan 31 03:42:40.947: %PLATFORM_POWER-6-MODEMISMATCH: Inline power not in Boost mode
Router(config)# exit
*Jan 31 03:36:13.111: %SYS-5-CONFIG_I: Configured from console by console
Router# show power
Main PSU :
Configured Mode : Boost
Current runtime state same : Yes
Total power available : 1450 Watts
POE Module :
Configured Mode : Boost
Current runtime state same : No
Total power available : 500 Watts
```

In this example, power for the main power supply is configured to be in boost mode by using the **no** form of the **power main redundant** command. This sets the power for the main power supply in boost mode to be 1450 W and the inline power in redundant mode as 500W.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# no power main redundant
Router(config)#
*Jan 31 03:35:22.284: %PLATFORM_POWER-6-MODEMATCH: Inline power is in Redundant mode
Router(config)#
Router(config)# exit
Router#
*Jan 31 03:36:13.111: %SYS-5-CONFIG_I: Configured from console by console
Router# show power
Main PSU :
Configured Mode : Boost
Current runtime state same : Yes
Total power available : 1450 Watts
POE Module :
Configured Mode : Redundant
Current runtime state same : Yes
Total power available : 500 Watts
Router#
```

Related Commands

Command	Description
show power inline	Displays the power status for the specified port or for all ports.
switchport priority extend	Determines how the telephone connected to the specified port handles priority traffic received on its incoming port.
switchport voice vlan	Configures the voice VLAN on the port.

power redundancy-mode

To set the power-supply redundancy mode, use the **power redundancy-mode** command in global configuration mode.

power redundancy-mode {**combined** | **redundant**}

Syntax Description

combined	Specifies no redundancy (combine power-supply outputs).
redundant	Specifies redundancy (either power supply can operate the system).

Command Default

redundant

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to set the power supplies to the no-redundancy mode:

```
Router(config)#
power redundancy-mode combined
Router(config)#
```

This example shows how to set the power supplies to the redundancy mode:

```
Router(config)#
power redundancy-mode redundant
Router(config)#
```

Related Commands

Command	Description
show power	Displays information about the power status.

ppp link

To generate the Point-to-Point Protocol (PPP) Link Control Protocol (LCP) down and keepalive-failure link traps or enable calls to the interface-reset vector, use the **ppplink**command in interface configuration mode. To disable the PPP LCP down and keepalive-failure link traps or calls to the interface-reset vector, use the **no** form of this command.

ppp link {**reset** | **trap**}
no ppp link {**reset** | **trap**}

Syntax Description

reset	Specifies calls to the interface reset vector.
trap	Specifies the PPP LCP down and keepalive-failure link traps.

Command Default

The defaults are as follows:

- The calls are sent to the interface-reset vector.
- The traps are sent when the LCP goes down.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720.

The **noppplinktrap** command disables the sending of the link traps when the LCP goes down.

In the event that the PPP calls the interface-reset vector while the LCP is configured or closed, Up/Down status messages will display on the console. If a leased-line configuration is up but the peer is not responding, PPP may call the interface-reset vector once per minute. This situation may result in the Up/Down status messages on the console. Use the **noppplinkreset**command to disable calls to the interface-reset vector. PPP will continue to attempt to negotiate with the peer, but the interface will not be reset between each attempt.

Examples

This example shows how to enable calls to the interface-reset vector:

```
Router(config-if)#
ppp link reset
Router(config-if)#
```

This example shows how to disable calls to the interface-reset vector:

```
Router(config-if)#
no ppp link reset
Router(config-if)#
```

This example shows how to generate the PPP LCP down/keepalive-failure link traps:

```
Router(config-if)#
ppp link trap
Router(config-if)#
```

This example shows how to disable the sending of the link traps when the LCP goes down:

```
Router(config-if)#
no ppp link trap
Router(config-if)#
```

ppp loopback no-backoff

To enable continuous Link Control Protocol (LCP) negotiation of loopback links with PPP sessions, use the **ppp loopback no-backoff** command in interface configuration mode. To restrict negotiation of loopback links with PPP sessions to ten LCP Configure Request (CONFREQ) messages, use the **no** form of this command.

ppp loopback no-backoff

no ppp loopback no-backoff

Command Default

Loopback links with PPP sessions disconnect after ten LCP CONFREQ messages are sent for negotiation.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.10.1S	This command was introduced.

Usage Guidelines

A circuit loopback indicates wiring issues in a device or faults with external switching equipment. The default functionality of the PPP protocol is to check for loopbacks and disconnect the session link when a loopback is detected. The PPP protocol includes a mechanism that detects a circuit loopback; that is, it detects a situation when a circuit feeds back upon itself, which results in the device reading its own output on that link. The first phase of loopback detection occurs during LCP negotiation when the circuit is being established. If you enable keepalives on a link, the second phase of loopback detection occurs after the connection is established.

Note Loopback detection depends upon successful negotiation of the LCP magic number during link establishment. LCP magic numbers are used in PPP to avoid frame loopbacks.

Use the **ppp loopback no-backoff** command when it becomes essential to prevent disconnection of session links whenever a loopback is detected. This ensures that the link does not go down and that there is a continuous attempt to establish connection. Link negotiations continue until a unique LCP magic number is received. The **no** form of this command restores the default behavior in which the loopback links with PPP sessions disconnect after only ten LCP CONFREQ messages are sent for negotiation.

Example

The following example shows how to enable the **ppp loopback no-backoff** command on a serial interface:

```
Device> enable
Device# configure terminal
Device(config)# interface Serial1/0/0:1
Device(config-if)# no ip address
Device(config-if)# encapsulation ppp
Device(config-if)# ppp loopback no-backoff
Device(config-if)# end
```

Related Commands

Command	Description
encapsulation ppp	Enables PPP on an interface.
no ip address	Removes an IP address or disables IP processing.
ppp loopback ignore	Disables PPP loopback detection.

ppp multilink mrru

To configure the maximum receive reconstructed unit (MRRU) value negotiated on a Multilink PPP (MLP) bundle, use the **pppmultilinkmrru**command in interface configuration mode. To remove the configured MRRU, use the **no** form of this command.

ppp multilink mrru [{**local** | **remote**}] **bytes**
no ppp multilink mrru [{**local** | **remote**}] **bytes**

Syntax Description

local	(Optional) Configures the local MRRU value.
remote	(Optional) Configures the minimum value that the software will accept from the peer when it advertises its MRRU.
bytes	MRRU value, in bytes. Valid value range is 128 to 16384.

Command Default

The default values for the local MRRU are the value of the multilink group interface maximum transmission unit (MTU) for multilink group members, and 1524 bytes for all other interfaces.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.0(28)S	This command was integrated into Cisco IOS Release 12.0(28)S.
12.2(27)SB	This command was integrated into Cisco IOS Release 12.2(27)SB.
12.2(28)S	This command was integrated into Cisco IOS Release 12.2(28)S.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.2(33)SRB1.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
15.2(2)SNI	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

This command allows the MRRU value to be configured on MLP interfaces and member links. This command is useful for interfaces running an application such as IP Security (IPsec), where the addition of the IPsec header causes the packet to exceed the 1500-byte MTU of a typical IP packet.

When using a large-bundle interface MTU size, you must ensure that the individual frames-per-fragment size passed to the link interfaces is not greater than the link interface MTU setting or the peer MRRU setting. This size limit can be achieved in one of the following two ways:

- Configure the link interface MTU setting appropriately.
- Configure fragmentation such that the link MTU settings will never be violated.

When MLP is configured, several physical interfaces can constitute one logical connection to the peer. To represent the logical connection, software provides a logical interface, often called the bundle interface. This interface will have the IP address, for instance, and the MTU setting of the interface that IP uses when it is deciding whether to fragment an IP datagram that needs to be forwarded. The physical interfaces forward individual MLP fragments or frames that are given to them by the bundle interface.

The result of having to decide whether to fragment a packet is that, whereas with simple PPP the interface MTU must not exceed the peer's MRRU, with MLP the MTU size of the bundle interface must not exceed the MRRU setting of the peer.

The MRRU settings on both sides need not be equal, but the "must not exceed" rule just specified must be followed; otherwise a system might send several fragments that, when reconstructed as a frame, will be too large for the peer's receive buffer.

Once you configure the MRRU on the bundle interface, you enable the router to receive large reconstructed MLP frames. You may want to configure the bundle MTU so that the router can send large MLP frames, although it is not strictly necessary. The maximum recommended value for the bundle MTU is the value of the peer's MTU. The software will automatically reduce the bundle interface MTU if necessary to avoid violating the peer's MRRU.

When the bundle interface MTU is tuned to a higher number, then depending upon the fragmentation configuration, the link interface may be given larger frames to send. There are two possible solutions to this problem, as follows:

- Ensure that fragmentation is performed such that fragments are sized less than the link interface MTU (refer to the command pages for the **pppmultilinkfragmentdisable** and **pppmultilinkfragmentdelay** commands for more information about packet fragments).
- Configure the MTUs of the link interfaces such that they can send the larger frames.

Note Be careful when configuring MLP MRRU negotiation in a virtual private dialup network (VPDN) environment when an L2TP network server (LNS) is not running Cisco IOS Release 12.3(7)T. The software performs strict matching on the MRRU values in earlier versions of Cisco IOS software.

Examples

The following example shows how to configure MRRU negotiation on a virtual template with synchronous serial interfaces. The example also applies to asynchronous serial interfaces.

```
multilink virtual-template 1
!
interface virtual-template 1
 ip address 10.13.1.1 255.255.255.0
 mtu 1600
!
interface serial 0/0
 ppp multilink
 ppp multilink mrru local 1600
 mtu 1600
!
interface serial 0/1
 ppp multilink
 ppp multilink mrru local 1600
```

mtu 1600

The following example shows how to configure MRRU negotiation on multilink groups:

```
interface multilink 10
 ip address 10.13.1.1 255.255.255.0
 ppp multilink mrru local 1600
 mtu 1600
!
interface serial 0/0
 ppp multilink
 multilink-group 10
 mtu 1600
!
interface serial 0/1
 ppp multilink
 multilink-group 10
 mtu 1600
```

The following example shows how to configure MRRU negotiation on dialer interfaces:

Note Dialer interfaces are not supported on the Cisco 7600 series router.

```
interface dialer 1
 ip address 10.13.1.1 255.255.255.0
 encapsulation ppp
 dialer remote-name 2610-2
 dialer idle-timeout 30 inbound
 dialer string 5550101
 dialer pool 1
 dialer-group 1
 no cdp enable
 ppp multilink
 ppp multilink mrru local 1600
```

Related Commands

Command	Description
encapsulation ppp	Sets the PPP encapsulation method.
interface dialer	Defines a dialer rotary group.
mtu	Adjusts the maximum packet size or MTU size.
multilink virtual-template	Specifies a virtual template from which the specified MLP bundle interface can clone its interface parameters.
ppp multilink	Enables MLP on an interface.
ppp multilink fragment delay	Specifies a maximum time for the transmission of a packet fragment on an MLP bundle.
ppp multilink fragment disable	Disables packet fragmentation.
ppp multilink fragmentation	Sets the maximum number of fragments a packet will be segmented into before being sent over the bundle.

Command	Description
ppp multilink group	Restricts a physical link to joining only a designated multilink-group interface.
ppp multilink interleave	Enables MLP interleaving.

pri-group

To specify ISDN PRI on a channelized E1 or T1 card on a Cisco 7500 series router, use the **pri-group** command in controller configuration mode. To remove the ISDN PRI, use the **no** form of this command.

pri-group commandpri-group [**timeslots** *range*]
no pri-group

Syntax Description

timeslots *range*	(Optional) Specifies a single range of values from 1 to 23.

Command Default

Disabled

Command Modes

Controller configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline or Technology-based releases. It may conintue to appear in Cisco IOS 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When you configure ISDN PRI, you must first specify an ISDN switch type for PRI and an E1 or T1 controller.

Examples

The following example specifies ISDN PRI on T1 slot 1, port 0:

```
Router# isdn switch-type primary-4ess
Router(config)# controllers t1 1/0
Router(config-controller)# framing esf
Router(config-controller)# linecode b8zs
Router(config-controller)# pri-group timeslots 2-6
```

Related Commands

Command	Description
controller	Configures a T1 or E1 controller and enters controller configuration mode.
interface serial	Specifies a serial interface created on a channelized E1 or channelized T1 controller (for ISDN PRI, CAS, or robbed-bit signaling).
isdn switch-type (PRI)	Specifies the central office switch type on the ISDN PRI interface.

priority1

To set a preference level for a Precision Time Protocol clock, use the **priority1** command in PTP clock configuration mode. To remove a priority1 configuration, use the **no** form of this command.

priority1 *priorityvalue*
no priority1 *priorityvalue*

Syntax Description

priorityvalue	Number value of the preference level. The range is from 0 to 255; lower values indicate a higher precedence. The default value is 128.

Command Default

The default preference level is 128.

Command Modes

PTP clock configuration (config-ptp-clk)

Command History

Release	Modification
15.0(1)S	This command was introduced.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

Subordinate devices use the priority1 value when selecting a primary clock. The priority1 value has precedence over the priority2 value.

Examples

The following example shows how to configure a ptp priority1 value:

```
Device> enable
Device# configure terminal
Device# ptp clock ordinary domain 0
Device(config-ptp-clk)# priority1 128
Device(config-ptp-clk)# end
```

Related Commands

Command	Description
priority2	Sets the PTP priority2 value.

priority2

To set a set a secondary preference level for a Precision Time Protocol clock, use the **priority2** command in PTP clock configuration mode. To remove a priority2 configuration, use the **no** form of this command.

priority2 *priorityvalue*
no priority2 *priorityvalue*

Syntax Description

priorityvalue	The number value of the preference level. The range is from 0 to 255; lower values indicate a higher precedence. The default value is 128.

Command Default

The default preference level is 128.

Command Modes

PTP clock configuration (config-ptp-clk)

Command History

Release	Modification
15.0(1)S	This command was introduced.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

Subordinate devices use the priority2 value to select a primary clock; the priority2 value is only considered when the device cannot use priority1 and other clock attributes to select a clock.

Examples

The following example shows how to configure the ptp priority2 value:

```
Device> enable
Device# configure terminal
Device# ptp clock ordinary domain 0
Device(config-ptp-clk)# priority2 128
Device(config-ptp-clk)# end
```

Related Commands

Command	Description
priority1	Sets the PTP priority1 value.

proactive enable

To enable automatic triggering of Forward Error Correction-Fast Re-Route (FEC-FRR), use the **proactive enable** command in DWDM configuration mode. To disable automatic triggering, use the no form of this command.

proactive enable

This command has no arguments or keywords.

Command Modes

DWDM Controller (config-controller)

Command History

Release	Modification
15.2(1)S	This command was introduced on the Cisco 7600 series routers.

Usage Guidelines

Examples

This example shows how to enable automatic triggering of Forward Error Correction-Fast Re-Route (FEC-FRR):

```
Router# configure terminal
Router(config)# controller dwdm 0/1
Router(config-controller)# proactive enable
```

Related Commands

Command	Description
proactive trig-threshold	Configures the trigger threshold of Forward Error Correction-Fast Re-Route (FEC-FRR).
proactive trig-window	Configures the trigger window (in milliseconds) in which Fast Re-Route may be triggered.
proactive rvrt-threshold	Configures the revert threshold to trigger reverting from the Forward Error Correction-Fast Re-Route (FEC-FRR) route back to the original route.
proactive rvrt-window	Configures the revert window in which reverting from the Forward Error Correction-Fast Re-Route (FEC-FRR) route back to the original route is triggered.

proactive rvrt-threshold

To configure the revert threshold to trigger reverting from the Forward Error Correction-Fast Re-Route (FEC-FRR) route back to the original route, use the **proactive rvrt-threshold** command in DWDM configuration mode. To remove the revert threshold, use the **no** form of this command.

proactive rvrt-threshold *x-coeff y-power*
no proactive rvrt-threshold *x-coeff y-power*

Syntax Description

x-coeff	Bit error rate coefficient (x of xE-y). The range is 1 to 9.
y-power	Bit error rate exponent (y of xE-y). The range is 3 to 9.

Command Default

Standard FEC mode: 1E-5

Enhanced FEC Mode: 1E-4

Command Modes

DWDM Controller (config-controller)

Command History

Release	Modification
15.2(1)S	This command was introduced on the Cisco 7600 series routers.

Examples

This example shows how to configure the revert threshold for FEC-FRR:

```
Router>enable
Router# configure terminal
Ruter(config)# controller dwdm 0/1
Router(config-controller)# proactive rvrt-threshold 1 6
```

Related Commands

Command	Description
proactive enable	Enables automatic triggering of Forward Error Correction-Fast Re-Route (FEC-FRR).
proactive trig-threshold	Configures the trigger threshold of Forward Error Correction-Fast Re-Route (FEC-FRR).
proactive trig-window	Configures the trigger window in which Fast Re-Route may be triggered.
proactive rvrt-window	Configures the revert window in which reverting from the Forward Error Correction-Fast Re-Route (FEC-FRR) route back to the original route is triggered.

proactive rvrt-window

To configure the revert window in which reverting from the Forward Error Correction-Fast Re-Route (FEC-FRR) route back to the original route is triggered, use the **proactive rvrt-window** command in DWDM configuration mode. To remove the revert window, use the no form of this command.

proactive rvrt-window *window*
no proactive rvrt-window *window*

Syntax Description

window	The length of time (in milliseconds) of the window in which reverting from FEC-FRR may be triggered. The range is 2000 to 100000.

Command Default

The default value of time is 2000.

Command Modes

DWDM configuration (config-controller)

Command History

Release	Modification
15.2(1)S	This command was introduced on the Cisco 7600 series routers.

Examples

This example shows how to configure the window in which reverting from FEC-FRR may be triggered:

```
Router# configure terminal
Router(config)# controller dwdm 0/1
Router(config-controller)# proactive rvrt-window 20345
```

Related Commands

Command	Description
proactive enable	Enables automatic triggering of Forward Error Correction-Fast Re-Route (FEC-FRR).
proactive trig-threshold	Configures the trigger threshold of Forward Error Correction-Fast Re-Route (FEC-FRR).
proactive trig-window	Configures the trigger window (in milliseconds) in which Fast Re-Route may be triggered.
proactive rvrt-threshold	Configures the revert threshold to trigger reverting from the Forward Error Correction-Fast Re-Route (FEC-FRR) route back to the original route.

proactive trig-threshold

To configure the trigger threshold of Forward Error Correction-Fast Re-Route (FEC-FRR), use the **proactive trig-threshold** command in DWDM configuration mode. To remove the trigger threshold, use the**no** form of this command.

proactive trig-threshold *x-coeff y-power*
no proactive trig-threshold *x-coeff y-power*

Syntax Description

x-coeff	Bit error rate coefficient (x of xE-y). The range is 1 to 9. Default is 1.
y-power	Bit error rate exponent (y of xE-y). The range is 3 to 9.

Command Default

Standard FEC mode: 6E-5

Enhanced FEC Mode: 6E-4

Command Modes

DWDM Controller (config-controller)

Command History

Release	Modification
15.2(1)S	This command was introduced on the Cisco 7600 series routers.

Examples

This example shows how to configure the trigger threshold of Forward Error Correction-Fast Re-Route (FEC-FRR).

```
Router# configure terminal
Router(config)# controller dwdm 0/1
Router(config-controller)#proactive trig-threshold 1 9
```

Related Commands

Command	Description
proactive enable	Enables automatic triggering of Forward Error Correction-Fast Re-Route (FEC-FRR).
proactive trig-window	Configures the trigger window (in milliseconds) in which Fast Re-Route may be triggered.
proactive rvrt-threshold	Configures the revert threshold to trigger reverting from the Forward Error Correction-Fast Re-Route (FEC-FRR) route back to the original route.

Command	Description
proactive rvrt-window	Configures the revert window in which reverting from the Forward Error Correction-Fast Re-Route (FEC-FRR) route back to the original route is triggered.

protection-group

Use this command to configure virtual protection group interface.

protection-group *group id type STS48c*

Syntax Description

Syntax Description:

group id	Identifier for the interface that is created
type	Protection group type It can be STS, STS3c, STS12c, and STS48c

Command Default

None

Command Modes

Controller configuration

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1	Support for this command was introduced for the Cisco NCS 4200 Series and Cisco ASR 900 Series Routers.

Usage Guidelines

This command is used for configuring protection group parameters.

Examples

The following example shows how to configure protection group:

```
enable
configure terminal
protection-group 401 type STS48c
controller protection group 401
type STS48c
cem-group 19001 cep
end
```

Related Commands

Command	Description
show protection-group	Verifies the protection group configuration.

protection-group [working | protect]

Use this command to configure protection group roles.

protection-group *group id* [**working** | **protect**]

Syntax Description

Syntax Description:

group id	Identifier for the interface that is created
working	The working interface for protection group
protect	The protect interface for protection group

Command Default

None

Command Modes

Controller configuration

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1	Support for this command was introduced for the Cisco NCS 4200 Series and Cisco ASR 900 Series Routers.

Usage Guidelines

Define the role either working interface or protect interface in the protection group.

Examples

The following example shows how to configure UPSR work path protection:

```
enable
configure terminal
controller mediatype 0/3/6
mode sonet
controller sonet 0/3/6
rate oc48
sts-1 1-48 mode sts-48c
protection-group 401 working
end
```

Related Commands

Command	Description
show protection-group	Verifies the protection group configuration.

protocol gre

To specify GRE as the tunnel mode and to set the GRE key for configuring the L3VPN encapsulation profile, use the **protocolgre** command in L3 VPN encapsulation configuration mode. To remove the transport source, use the **no** form of this command.

protocol gre [**key** *gre key*]
no protocol [**gre**]

Syntax Description

key	(Optional) Specifies the key for GRE tunnel interface.
gre key	(Optional) The GRE key value. The range is from 0 to 4294967295.

Command Default

The tunnel mode and GRE key are not specified.

Command Modes

L3VPN Encapsulation Configuration (config-l3vpn-encap-ip)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.

Examples

The following example shows how to specify GRE as the tunnel mode and to set the GRE key:

```
Router(config-l3vpn-encap-ip)# protocol gre key 500
```

Related Commands

Command	Description
l3vpn encapsulation ip	Configures the L3VPN encapsulation profile.
transport ipv4	Specifies IPv4 transport source mode and the transport source interface.
show l3vpn encapsulation ip	Displays the profile health and the underlying tunnel interface.

ptp clock

To create a Precision Time Protocol clock and specify the clock mode, use the **ptpclock** command in the global configuration mode. To remove a ptp clock configuration, use the **no** form of this command.

ptp clock {**ordinary** | **transparent**} **boundary domain** *domain*
no ptp clock {**ordinary** | **transparent**} **boundary domain** *domain*

Syntax Description

ordinary	Sets the PTP clock to ordinary clocking mode.
transparent	Sets the PTP clock to transparent clock mode; the router modifies outgoing PTP sync and delay-request messages to account for residence time using the correction field in the follow-up message.
boundary	Sets the PTP clock to boundary clock mode; the router participates in selecting the best master clock and can act as the master clock if no better clocks are detected.
domain	The PTP clocking domain number. Valid values are from 0 to 127.

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)S	This command was introduced.

Usage Guidelines

This command creates a new PTP clock and enters clock configuration mode.

Examples

The following example shows how to configure a PTP clock and enter clock configuration mode:

```
Router# configure terminal
Router# ptp clock ordinary domain 0
Router(config-ptp-clk)#
```

Related Commands

Command	Description
clock-port	Specifies the mode of a PTP clock port.

pulse-time

To enable pulsing data terminal ready (DTR) signal intervals on the serial interfaces, use the **pulse-time** command in interface configuration mode. To restore the default interval, use the **no** form of this command.

pulse-time[{**msec***seconds*}]
no pulse-time

Syntax Description

msec	(Optional) Specifies the use of milliseconds for the DTR signal interval.
seconds	Integer that specifies the DTR signal interval in seconds. If the **msec** keyword is configured, the DTR signal interval is specified in milliseconds. The default is 0.

Command Default

0 seconds

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.1(5)T	The optional **msec** keyword was added to configure the interval in milliseconds.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When the serial line protocol goes down (for example, because of loss of synchronization), the interface hardware is reset and the DTR signal is held inactive for at least the specified interval. This function is useful for handling encrypting or other similar devices that use the toggling of the DTR signal to resynchronize.

Use the optional **msec** keyword to specify the DTR signal interval in milliseconds. A signal interval set to milliseconds is recommended on High-Speed Serial Interfaces (HSSIs).

Note

Whenever the **pulse-time** command is configured for the synchronous serial interface, do one of the following after every interface state transition. This ensures that the DTR is pulsed down for the configured interval:

- In exec mode, issue the **clear interface serial** *x*/*y*/[*z*] command.
- In config mode of the serial interface, issue a **shutdown**, followed by **no shutdown**.

If you do not clear/reset the interface with one of these procedures, the **pulse-time** command will have no effect.

Optionally, you can automate this procedure using an EEM or Tcl script. The following example EEM script clears the serial interface after a disconnection:

```
event manager applet CLEAR_INIT_S000
 event syslog pattern "Line protocol on Interface Serial0/0/0, changed state to down"
 action 2.0 cli command "enable"
 action 2.1 cli command "clear int Serial0/0/0"
 action 3.0 syslog msg "clear int Serial0/0/0"
```

Examples

The following example enables DTR pulse signals for 3 seconds on serial interface 2:

```
Router(config)# interface serial 2
Router(config-if)# pulse-time 3
```

The following example enables DTR pulse signals for 150 milliseconds on HSSI interface 2/1/0:

```
Router(config)# interface hssi 2/1/0
Router(config-if)# pulse-time msec 150
```

rate

Use this command to enable the rate for SONET and SDH ports.

For SONET:

rate [*OC3* | *OC12* | *OC48* | *OC192*

For SDH:

rate [*STM-1* | *STM-4* | *STM-16* | *STM-64*

Syntax Description

Syntax Description:

OC3	Configures OC-3 port.
OC12	Configures OC-12 port.
OC-48	Configures OC-48 port.
OC-192	Configures OC-192 port.
STM-1	Configures STM-1 port.
STM-4	Configures STM-4 port.
STM-16	Configures STM-16 port.
STM-64	Configures STM-64 port.

Command Default

None

Command Modes

Controller configuration

Command History

Release	Modification
XE 3.18SP	Support for this command was introduced on NCS 4200 Series for SONET.
XE Everest 16.6.1	This command was integrated into the Cisco NCS 4200 Series and Cisco ASR 900 Series for SDH.

Usage Guidelines

Configuration of this command is mandatory.

Examples

The following example shows how to configure Mediatype controller mode:

```
enable
configure terminal
controller MediaType 0/5/0
mode sonet
controller sonet 0/5/0
rate oc3
end
```

To configure mode VC4 CEP:

```
enable
configure terminal
controller sdh 0/5/0
rate stm 4
aug mapping au-4
au-4 1
mode vc4
cem-group 100 cep
end
```

Related Commands

Command	Description
controller sonet	Configures the SONET mode.
show controller sonet	Displays SONET controller configuration.

recovered-clock

To configure an associated clock ID with the corresponding CEM circuit, use the **recovered-clock** command in global configuration mode.

recovered-clock *bay slot*

Syntax Description

bay	Identifies the bay where the CEM circuit is inserted. On NCS4200 series bay value is 0 always.
slot	Physical slot number. The slot number is in a range either from 0 to 5 or 8 to 13, depending on the slot in which the STM-1 card resides. The slot is always 0 for Cisco NCS 4200 Series. The physical slot ranges from 0 to 5 for Cisco ASR 900 Series Routers. The value of physical slot supported for Cisco ASR 920 Routers is 1.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
XE 3.18SP	This command was integrated into Cisco NCS 4200 Series
XE Everest 16.5.1	This command was integrated into Cisco NCS 4200 Series. This command was introduced into Cisco ASR 900 Series routers.

Usage Guidelines

This command will be used when the clock needs to be recovered by the same CEM circuit.

The following example shows how to configure an associated clock ID with the corresponding CEM circuit.

```
recovered-clock 0 3
 clock recovered 1 differential cem 0 1
```

Related Commands

Command	Description
clock recovered adaptive/differential cem	Associates the clock recovered ID to the CEM group.

redundancy

To enter redundancy configuration mode, use the **redundancy**command in global configuration mode. This command does not have a **no** form.

redundancy

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(5)XV1	This command was introduced on the Cisco AS5800 universal access server.
12.2(4)XF	This command was introduced for the Cisco uBR10012 router.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
12.0(9)SL	This command was integrated into Cisco IOS Release 12.0(9)SL.
12.0(16)ST	This command was implemented on the Cisco 7500 series Internet routers.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)SX	Support for this command was added for the Supervisor Engine 720.
12.2(18)S	This command was implemented on the Cisco 7500 series Internet routers.
12.2(20)S	This command was implemented on the Cisco 7304 router.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.3(7)T	This command was implemented on the Cisco 7500 series Internet routers.
12.2(8)MC2	This command was implemented on the MWR 1900 Mobile Wireless Edge Router (MWR).
12.3(11)T	This command was implemented on the MWR 1900 MWR.
12.3BC	This command was integrated into Cisco IOS Release 12.3BC.
12.0(22)S	This command was implemented on the Cisco 10000 series Internet routers.
12.2(18)SXE2	This command was integrated into Cisco IOS Release 12.2(18)SXE2.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(44)SQ	This command was integrated into Cisco IOS Release 12.2(44)SQ. Support for the Cisco RF Gateway 10 was added.

Release	Modification
12.2(33) SRE	This command was modified. The interchassis subconfiguration mode was added.

Usage Guidelines

Use the **redundancy** command to enter redundancy configuration mode, where you can define aspects of redundancy such as shelf redundancy for the Cisco AS5800 universal access server.

Cisco 10000 Series Router

Before configuring line card redundancy, install the Y-cables. Before deconfiguring redundancy, remove the Y-cables.

The following restrictions apply to line card redundancy on the Cisco 10000 series router:

- Port-level redundancy is not supported.
- Redundant cards must occupy the two subslots within the same physical line card slot.
- The line card that will act as the primary line card must be the first line card configured, and it must occupy subslot 1.

Cisco 7600 Series Router

From redundancy configuration mode, you can enter the main CPU submode to manually synchronize the configurations that are used by the two supervisor engines.

From the main CPU submode, you can use the **auto-sync** command to use all the redundancy commands that are applicable to the main CPU.

To select the type of redundancy mode, use the **mode** command.

Nonstop forwarding (NSF) with stateful switchover (SSO) redundancy mode supports IPv4. NSF with SSO redundancy mode does not support IPv6, Internetwork Packet Exchange (IPX), and Multiprotocol Label Switching (MPLS).

After you enter redundancy configuration mode, you can use the **interchassis** command to specify the redundancy group number and enter interchassis redundancy mode. In the interchassis redundancy configuration mode, you can do the following:

- Specify a backbone interface for the redundancy group using the **backbone** command.
- Exit from interchassis configuration mode using the **exit** command.
- Specify the IP address of the remote redundancy group member using the **member ip** command.
- Specify the multichassis LACP (mLACP) node ID, system MAC address, and system priority using the **node-id**, **system-mac**, and **system-priority** commands.
- Define the peer monitoring method using the **monitor** command.

Cisco uBR10012 Universal Broadband Router

After you enter redundancy configuration mode, you can use the **main-cpu** command to enter main-CPU redundancy configuration mode, which allows you to specify which files are synchronized between the active and standby Performance Routing Engine (PRE) modules.

Cisco RF Gateway 10

At the redundancy configuration mode, you can do the following:

- Set a command to its default mode using the **default** command.
- Exit from a redundancy configuration using the **exit** command.
- Enter the line card group redundancy configuration using the **linecard-group** command.
- Enter main-CPU redundancy configuration mode using the **main-cpu** command, which allows you to specify which files are synchronized between the active and standby Supervisor cards.
- Configure the redundancy mode for the chassis using the **mode** command.
- Enforce a redundancy policy using the **policy** command.

Examples

The following example shows how to enable redundancy mode:

```
Router(config)# redundancy
Router(config-red)#
```

The following example shows how to assign the configured router shelf to the redundancy pair designated as 25. This command must be issued on both router shelves in the redundant router-shelf pair:

```
Router(config)# redundancy
Router(config-red)# failover group-number 25
```

Cisco 10000 Series Router

The following example shows how to configure two 4-port channelized T3 half eight line cards that are installed in line card slot 2 for one-to-one redundancy:

```
Router(config)# redundancy
Router(config-r)# linecard-group 1 y-cable
Router(config-r-lc)# member subslot 2/1 primary
Router(config-r-lc)# member subslot 2/0 secondary
```

Cisco 7600 Series Router

The following example shows how to enter the main CPU submode:

```
Router(config)#
redundancy
Router(config-r)#
main-cpu
Router(config-r-mc)#
```

Cisco uBR10012 Universal Broadband Router

The following example shows how to enter redundancy configuration mode and display the commands that are available in that mode on the Cisco uBR10012 router:

```
Router# configure terminal
```

```
Router(config)# redundancy

Router(config-r)# ?

Redundancy configuration commands:
  associate  Associate redundant slots
  exit       Exit from redundancy configuration mode
  main-cpu   Enter main-cpu mode
  no         Negate a command or set its defaults
```

The following example shows how to enter redundancy configuration mode and displays its associated commands on the Cisco RFGW-10 chassis:

```
Router# configure terminal
Router(config)# redundancy
Router(config-r)#?
Redundancy configuration commands:
  default         Set a command to its defaults
  exit            Exit from redundancy configuration mode
  linecard-group  Enter linecard redundancy submode
  main-cpu        Enter main-cpu mode
  mode            redundancy mode for this chassis
  no              Negate a command or set its defaults
  policy          redundancy policy enforcement
```

The following example shows how to enter redundancy configuration mode and its associated commands in the interchassis mode:

```
Router# configure terminal
Router(config)# redundancy
```

Router(config-r)#?

```
Redundancy configuration commands:
  exit          Exit from redundancy configuration mode
  interchassis  Enter interchassis mode
  no            Negate a command or set its defaults
Router(config-r)# interchassis group 100

R1(config-r-ic)# ?
Interchassis redundancy configuration commands:
  backbone  specify a backbone interface for the redundancy group
  exit      Exit from interchassis configuration mode
  member    specify a redundancy group member
  mlacp     mLACP interchassis redundancy group subcommands
  monitor   define the peer monitoring method
  no        Negate a command or set its defaults
```

Related Commands

Command	Description
associate slot	Logically associates slots for APS processor redundancy.
auto-sync	Enables automatic synchronization of the configuration files in NVRAM.
clear redundancy history	Clears the redundancy event history log.
linecard-group y-cable	Creates a line card group for one-to-one line card redundancy.

Command	Description
main-cpu	Enters main-CPU redundancy configuration mode for synchronization of the active and standby PRE modules or Supervisor cards.
member subslot	Configures the redundancy role of a line card.
mode (redundancy)	Configures the redundancy mode of operation.
redundancy force-switchover	Switches control of a router from the active RP to the standby RP.
show redundancy	Displays information about the current redundant configuration and recent changes in states or displays current or historical status and related information on planned or logged handovers. In the redundancy configuration of Cisco ASR 920 Series Routers, the commands related to MR-APS feature are only supported.

redundancy all-active replicate

To enable all-active pseudowire redundancy mode with traffic replication, use the **redundancy all-active replicate** command in global or interface configuration mode. To disable this functionality, use the **no** form of this command.

redundancy all-activereplicate
no redundancy all-activereplicate

Syntax Description

replicate	Replicates the pseudowire state on the router.

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.18.1SP	This command was introduced on the Cisco ASR 900 Series Routers.

Usage Guidelines

The **redundancy all-active replicate** command maintains the working ad protect pseudowires in a pseudowire redundancy configuration with MR-APS configuration to remain in the UP state.

Examples

The following example shows the configuration at global level:

```
pseudowire-class 2G-PW
encapsulation mpls
status peer topology dual-homed

controller E1 0/1
framing unframed
cem-group 8 unframed
```

The following examples shows the configuration at interface level:

```
interface CEM0/1
no ip address
cem 8
xconnect 10.10.10.1 8 encapsulation mpls pw-class 2G-PW
backup peer 10.10.10.2 8 pw-class 2G-PW
redundancy all-active replicate
```

Related Commands

Command	Description
pseudowire class	Configures the pseudowire class on the router.
template typepseudowire	Configures the pseudowire template on the router.

redundancy force-switchover

To force the standby Route Processor (RP) or Supervisor card to assume the role of the active RP or Supervisor card, use the **redundancy force-switchover** command in privileged EXEC mode.

redundancy force-switchover [**main-cpu**]

Syntax Description

main-cpu	(Optional) Forces switchover to the main CPU.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(16)ST	This command was introduced.
12.1(10)EX2	This command was integrated into Cisco IOS Release 12.1(10)EX2.
12.0(17)ST	This command was implemented on the Cisco 12000 series routers.
12.0(22)S	This command replaces the **force-failover**command on the Cisco 10000 series routers.
12.2(14)SX	Support for this command was added for the Supervisor Engine 720.
12.2(18)S	This command was implemented on the Cisco 7500 series routers.
12.2(20)S	Support was added for the Cisco 7304 router.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.
12.2(44)SQ	This command was integrated into Cisco IOS Release 12.2(44)SQ. Support for the Cisco RF Gateway 10 was added.

Usage Guidelines

Use the **redundancy force-switchover** command to switch control of a router from the active RP or Supervisor card to the standby RP or Supervisor card. Both the active and standby RPs or Supervisor cards must have a high availability Cisco IOS image installed and must be configured for Route Processor Redundancy (RPR) mode before the **redundancy force-switchover** command can be used. Before the system switches over, it verifies that the standby RP or Supervisor card is ready to take over.

When you use the **redundancy force-switchover**command and the current running configuration is different from the startup configuration, the system prompts you to save the running configuration before the switchover is performed.

Note All line cards will reset in RPR mode on a switchover.

Note Before using this command in Cisco 7600 series routers, refer to the "Performing a Fast Software Upgrade" section of the *Cisco 7600 Series Router Cisco IOS Software Configuration Guid*e for additional information.

On Cisco 7600 series routers, the **redundancy force-switchover** command conducts a manual switchover to the redundant supervisor engine. The redundant supervisor engine becomes the new active supervisor engine running the new Cisco IOS image. The modules are reset and the module software is downloaded from the new active supervisor engine.

The active and redundant supervisor engines do not reset on a Route Processor Redundancy Plus (RPR+) switchover. The old active supervisor engine reboots with the new image and becomes the redundant supervisor engine.

Beginning with Cisco IOS Release 12.2(33)SCA, you can force a Performance Routing Engine (PRE) switchover using the **redundancy force-switchover main-cpu** command from either the primary or standby PRE. If you force a switchover from the active PRE, both PREs synchronize and the active PRE reloads normally. When you force a switchover from the standby PRE, a crash dump of the active PRE occurs for troubleshooting purposes. Forcing a switchover from the standby PRE should only be done if you cannot access the active PRE.

Examples

The following example shows a switchover from the active RP to the standby RP on a Cisco 7513 router with RPR configured:

```
Router# configure terminal
Router(config)# hw-module slot 7 image slot0:rsp-pv-mz
Router(config)# hw-module slot 6 image slot0:rsp-pv-mz
Router(config)# slave auto-sync config
Router(config)# redundancy
Router(config-r)# mode rpr
Router(config-r)# end
Router# copy running-config startup-config
Router# redundancy force-switchover
```

The following example shows how to perform a manual switchover from the active to the standby RP when the running configuration is different from the startup configuration:

```
Router# redundancy force-switchover
System configuration has been modified. Save? [yes/no]:y
Building configuration...
...
...
[OK]
Proceed with switchover to standby NSE? [confirm]y
00:07:35:%SYS-5-SWITCHOVER:Switchover requested
```

The following example shows how to perform a manual switchover from the active to the standby RP when the running configuration is the same as the startup configuration:

```
Router# redundancy force-switchover
Proceed with switchover to standby NSE? [confirm]
00:07:35:%SYS-5-SWITCHOVER:Switchover requested
```

Cisco RF Gateway 10

The following example shows how to perform a manual switchover from the active to the standby RP when the running configuration is different from the startup configuration:

```
Router# redundancy force-switchover
System configuration has been modified. Save? [yes/no]:y
Building configuration...
...
...
[OK]
Proceed with switchover to standby NSE? [confirm]y
00:07:35:%SYS-5-SWITCHOVER:Switchover requested
```

The following example shows how to perform a manual switchover from the active to the standby RP when the running configuration is the same as the startup configuration:

```
Router# redundancy force-switchover
Proceed with switchover to standby NSE? [confirm]
00:07:35:%SYS-5-SWITCHOVER:Switchover requested
```

Related Commands

Command	Description
clear redundancy history	Clears the redundancy event history log.
hw-module sec-cpu reset	Resets and reloads the standby RP with the specified Cisco IOS image and executes the image.
hw-module slot image	Specifies a high availability Cisco IOS image to run on an active or standby RP.
mode (HSA redundancy)	Configures the High System Availability (HSA) redundancy mode.
mode (redundancy)	Configures the redundancy mode of operation.
redundancy	Enters redundancy configuration mode.
show redundancy	Displays current active and standby Performance Routing Engine (PRE) redundancy status.

redundancy handover

To hand over control of resources (slots and cards) from a route-switch-controller (RSC) card to its peer RSC card, use the **redundancyhandover** command in privileged EXEC mode.

redundancy handover {**cancel** | {**peer-resources** | **shelf-resources**} [**busyout-period** *mins*] [**at** *hh* **:** *mm* [{*day month* | *month day*} *year*]]}

Syntax Description

cancel	Any pending handover is canceled.
peer-resources	Resources to be handed over are those on the side of the peer RSC. This parameter applies only when the system is in extraload.
shelf-resources	Resources to be handed over are those on the side of the RSC from which the command is run.
busyout-period *mins*	(Optional) Time period for which all slots in the selected resources are to be busied out before handover. If time options are omitted, handover or busyout period begins immediately.
at *hh* **:** *mm day month year*	(Optional) Time of the handover or start of the busyout period, in 24-hour time format; hour and minute are required; day, month, and year are optional.

Command Default

Control remains with the assigned RSC.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)XB1	This command was introduced.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

To use this command, you must have two RSC cards installed on your Cisco AS5850 and you must be connected to one of them in handover-split mode. This command can be run from either RSC and can specify that slots be handed over to the peer RSC.

After handover and subsequent restoration of the failed RSC, connect to the active RSC and use this command to return control of cards to the previously failed but now restored RSC.

Note that when you enter the command with the **shelf-resources** option, the RSC reloads.

Examples

The following example hands over control, to the peer RSC, of the slots and cards on the corresponding side of the chassis. Note the prompt to confirm clearing of calls, handover, and reload on the last line.

```
Router# redundancy handover shelf-resources busyout-period 10 at 22:00 3 Sep 2005

Newly entered handover schedule:
Busyout period at 22:00:00 PDT Sat Sep 3 2005 for a duration of 10 minutes
```

```
Handover pending at 22:10:00 PDT Sat Sep 3 2005
Clear calls, handover and reload as specified above? y
```

Related Commands

Command	Description
show redundancy debug-log	Displays up to 256 relevant debug entries.
show redundancy handover	Displays details of any pending handover (that is, a handover command that was entered previously and is not yet completed).
show redundancy history	Displays logged handover events.

redundancy stateful

To configure stateful failover for tunnels using IP Security (IPSec), use the **redundancystateful**command in crypto map configuration mode. To disable stateful failover for tunnel protection, use the **no** form of this command.

redundancy *standby-group-name* **stateful**
no redundancy *standby-group-name* **stateful**

Syntax Description

standby-group-name	Refers to the name of the standby group as defined by Hot Standby Router Protocol (HSRP) standby commands. Both routers in the standby group are defined by this argument and share the same virtual IP (VIP) address.

Command Default

Stateful failover is not enabled for IPSec tunnels.

Command Modes

Crypto map configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

The **redundancystateful**command uses an existing IPSec profile (which is specified via the **cryptoipsecprofile**command) to configure IPSec stateful failover for tunnel protection. (You do not configure the tunnel interface as you would with a crypto map configuration.) IPSec stateful failover enables you to define a backup IPSec peer (secondary) to take over the tasks of the active (primary) router if the active router is deemed unavailable.

The tunnel source address must be a VIP address, and it must not be an interface name.

Examples

The following example shows how to configure stateful failover for tunnel protection:

```
crypto ipsec profile peer-profile
  redundancy HA-out stateful

interface Tunnel1
 ip unnumbered Loopback0
 tunnel source 209.165.201.3
 tunnel destination 10.0.0.5
 tunnel protection ipsec profile peer-profile
!
interface Ethernet0/0
 ip address 209.165.201.1 255.255.255.224
 standby 1 ip 209.165.201.3
 standby 1 name HA-out
```

Related Commands

Command	Description
crypto ipsec profile	Defines the IPSec parameters that are to be used for IPSec encryption between two routers and enters crypto map configuration mode.

remote command

To execute a Cisco 7600 series router command directly on the switch console or a specified module without having to log into the Cisco 7600 series router first, use the **remote command** command in privileged EXEC mode.

remote command {**module** *num* | **standby-rp** | **switch**} *command*

Syntax Description

module *num*	Specifies the module to access; see the “Usage Guidelines” section for valid values.
standby-rp	Specifies the standby route processor.
switch	Specifies the active switch processor.
command	Command to be executed.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXD	The **standby-rp** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **module** *num* keyword and argument designate the module number. Valid values depend on the chassis that is used. For example, if you have a 13-slot chassis, valid values are from 1 to 13. The **module** *num* keyword and argument are supported on DFC-equipped modules and the standby supervisor engine only.

When you execute the **remote command switch**command, the prompt changes to Switch-sp#.

This command is supported on DFC-equipped modules and the supervisor engine only.

This command does not support command completion, but you can use shortened forms of the command (for example, entering **sh** for **show**).

Examples

This example shows how to execute the **show calendar** command from the standby route processor:

```
Router#
remote command standby-rp show calendar
Switch-sp#
09:52:50 UTC Mon Nov 12 2001
Router#
```

Related Commands

Command	Description
remote login	Accesses the Cisco 7600 series router console or a specific module.

remote-span

To configure a virtual local area network (VLAN) as a remote switched port analyzer (RSPAN) VLAN, use the **remote-span** command in config-VLAN mode. To remove the RSPAN designation, use the **no** form of this command.

remote-span
no remote-span

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Config-VLAN mode

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported in the VLAN database mode.

You can enter the **show vlan remote-span** command to display the RSPAN VLANs in the Cisco 7600 series router.

Examples

This example shows how to configure a VLAN as an RSPAN VLAN:

```
Router(config-vlan)# remote-span
Router(config-vlan)
```

This example shows how to remove the RSPAN designation:

```
Router(config-vlan)# no remote-span
Router(config-vlan)
```

Related Commands

Connect	Description
show vlan remote-span	Displays a list of RSPAN VLANs.

remote login

To access the Cisco 7600 series router console or a specific module, use the **remote login** command in privileged EXEC mode.

remote login {**module** *num* | **standby-rp** | **switch**}

Syntax Description

module *num*	Specifies the module to access; see the "Usage Guidelines" section for valid values.
standby-rp	Specifies the standby route processor.
switch	Specifies the active switch processor.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXD	This command was changed to include the **standby-rp** keyword.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Caution When you enter the **attach** or **remote login** command to access another console from your switch, if you enter global or interface configuration mode commands, the switch might reset.

The **module** *num* keyword and argument designate the module number. Valid values depend on the chassis that is used. For example, if you have a 13-slot chassis, valid values are from 1 to 13. The **module** *num* keyword and argument are supported on DFC-equipped modules and the standby supervisor engine only.

When you execute the **remote login module** *num* command, the prompt changes to Router-dfcx# or Switch-sp#, depending on the type of module to which you are connecting.

When you execute the **remote login standby-rp** command, the prompt changes to Router-sdby#.

When you execute the **remote login switch** command, the prompt changes to Switch-sp#.

The **remote login module** *num* command is identical to the **attach** command.

There are two ways to end the session:

- You can enter the **exit** command as follows:

```
Switch-sp# exit
```

```
[Connection to Switch closed by foreign host]
Router#
```

- You can press **Ctrl-C** three times as follows:

```
Switch-sp# ^C
Switch-sp# ^C
Switch-sp# ^C
Terminate remote login session? [confirm] y
[Connection to Switch closed by local host]
Router#
```

Examples

This example shows how to perform a remote login to a specific module:

```
Router# remote login module 1
Trying Switch ...
Entering CONSOLE for Switch
Type "^C^C^C" to end this session
Switch-sp#
```

This example shows how to perform a remote login to the Cisco 7600 series router processor:

```
Router# remote login switch
Trying Switch ...
Entering CONSOLE for Switch
Type "^C^C^C" to end this session
Switch-sp#
```

This example shows how to perform a remote login to the standby route processor:

```
Router# remote login standby-rp
Trying Switch ...
Entering CONSOLE for Switch
Type "^C^C^C" to end this session
Router-sdby#
```

Related Commands

Command	Description
attach	Connects to a specific module from a remote location.

reset (alarm-interface)

To reset the CPU in the alarm interface controller (AIC), use the **reset**command in alarm-interface mode.

reset

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Alarm-interface

Command History

Release	Modification
12.2(2)XG	This command was introduced on the Cisco 2600 series and Cisco 3600 series.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

A change in the AIC IP configuration might not take effect until the next time the card is started. Use the **reset** command to restart the card. This command does not have a **no** form.

Examples

The following example shows a message that might be returned after the **reset** command is entered:

```
Router(alarm-aic)# reset
Selected card in slot 1 restarted
```

Related Commands

Command	Description
alarm-interface	Enters alarm-interface mode and configures the AIC.

retry

To define the amount of time that must elapse before a connection is attempted to a failed server, use the **retry** command in interface configuration mode. To change the connection-reassignment threshold and client threshold to the default settings, use the **no** form of this command.

retry *retry-value*
no retry

Syntax Description

retry-value	Amount of time, in seconds, that must elapse after the detection of a server failure before a new connection is attempted to the server; valid values are from 1 to 3600.

Command Default

retry-value is **60**

Command Modes

real server configuration submode

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to specify a retry timer of 30 seconds:

```
Router(config)# ip slb serverfarm serverfarm-name
Router(config-slb-sfarm)# real 10.1.1.1
Cisco-7600(config-slb-real)# retry 30
```

This example shows how to revert to the default value:

```
Cisco-7600(config-slb-real)# no
 retry
Router(config-if)#
```

Related Commands

Command	Description
faildetect numconns	Specifies the conditions that indicate a server failure.
inservice (real server)	Enables the real server for use by the IOS SLB feature.
maxconns	Limits the number of active connections to the real server.

ring-speed

To set the ring speed for the CSC-1R and CSC-2R Token Ring interfaces, use the **ring-speed** command in interface configuration mode.

ring-speed commandring-speed *speed*

Syntax Description

speed	Integer that specifies the ring speed, either 4 for 4-Mbps operation or 16 for 16-Mbps operation . The default is 16.

Command Default

16-Mbps operation

Caution Configuring a ring speed that is wrong or incompatible with the connected Token Ring causes the ring to beacon, which makes the ring nonoperational.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command does not have a **no** form.

Examples

The following example shows how to sets the ring speed to 4 Mbps on a Token Ring interfaces:

```
Router(config)# interface tokenring 0
Router(config-if)# ring-speed 4
```

rj45-auto-detect-polarity

To enable or disable polarity detection for 10 Mbps full-duplex links, use the **rj45-auto-detect-polarity** command in interface configuration mode.

rj45-auto-detect-polarity {**enable** | **disable**}

Syntax Description

enable	Enables polarity detection on the RJ45 interface.
disable	Disables polarity detection on the RJ45 interface.

Command Default

Polarity detection is disabled for 10 Mbps, full duplex links.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.0(1)M3	This command was introduced.

Usage Guidelines

This command is available only for 10 Mbps, full-duplex links. The polarity detection feature helps to detect reversed polarity and provide correction; however, there is a risk of cyclic redundancy check (CRC) errors if polarity detection is enabled.

The polarity detection feature is disabled by default. Use the **rj45-auto-detect-polarityenable**to enable polarity detection.

It is recommended to leave polarity detection disabled.

Examples

The following example shows how to enable polarity detection on the RJ45 interface:

```
router(config-if)# rj45-auto-detect-polarity enable
```

Related Commands

Command	Description
media-type auto-failover	Assigns the RJ45 or the SFP port as the primary and secondary failover media.

scramble through service-module t1 lbo

scramble

To enable scrambling (encryption) of the payload on a T3 or E3 controller or on the PA-T3 and PA-E3 port adapters, use the **scramble** command in interface configuration mode. To disable scrambling, use the **no** form of this command.

scramble
no scramble

Syntax Description

This command has no arguments or keywords.

Command Default

Scrambling is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.1CA	This command was introduced.
12.2(11)YT	This command was integrated into Cisco IOS Release 12.2(11)YT and implemented on the following platforms: Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3660 series, Cisco 3725, and Cisco 3745 routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

T3/E3 scrambling is used to assist clock recovery on the receiving end. Scrambling is designed to randomize the pattern of 1s and 0s carried in the physical layer frame. Randomizing the digital bits can prevent continuous, nonvariable bit patterns--in other words, long strings of all 1s or all 0s. Several physical layer protocols rely on transitions between 1s and 0s to maintain clocking.

Scrambling can prevent some bit patterns from being mistakenly interpreted as alarms by switches placed between the Data Service Units (DSUs).

The local interface configuration must match the remote interface configuration. For example, if you enable scrambling on the local port, you must also do the same on the remote port.

To verify that scrambling is configured on the interface, use the **showcontrollersserial**or the **showinterfacesserial**commands.

For T3 controllers, all the DSU modes support scrambling except Clear mode.

For E3 controllers, only Kentrox mode supports scrambling.

Examples

The following example enables scrambling on the PA-E3 port adapter in slot 1, port adapter slot 0, interface 0:

```
Router(config)# interface serial 1/0/0
Router(config-if)# scramble
```

The following example enables scrambling on the controller in slot 1, port 0:

```
Router(config)# interface serial 1/0
Router(config-if)# scramble
```

Related Commands

Command	Description
show controllers serial	Displays information that is specific to the serial controllers.
show interfaces serial	Displays information that is specific to the interface hardware.

serial restart-delay

To set the amount of time that the router waits before trying to bring up a serial interface when it goes down, use the **serialrestart-delay** command in interface configuration mode. To restore the default, use the **no** form of the command.

serial restart-delay *count*
no serial restart-delay

Syntax Description

count	Frequency, in milliseconds, at which the hardware is reset. Range is from 0 to 900. Default is 0.

Command Default

0 milliseconds

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.2 P	This command was introduced.
12.2(4)T	The *count* value was changed to set time in milliseconds rather than in seconds.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(2)S	This command was integrated into Cisco IOS Release 15.1(2)S.

Usage Guidelines

The router resets the hardware each time the serial restart timer expires. This command is often used with the dial backup feature and with the **pulse-time** command, which sets the amount of time to wait before redialing when a DTR dialed device fails to connect.

When the*count*value is set to the default of 0, the hardware is not reset when it goes down. In this way, if the interface is used to answer a call, it does not cause DTR to drop, which can cause a communications device to disconnect.

Examples

The following example shows how to set the restart delay on serial interface 0 to 0:

```
Router(config)# interface serial 0
Router(config-if)# serial restart-delay 0
```

Related Commands

Command	Description
pulse-time	Enables pulsing DTR signal intervals on the serial interfaces.
show interfaces serial	Displays information about a serial interface.

server ip address

To configure a static IP address for the Cisco E-Series Server, use the **server ip address** command in interface configuration mode.

server ip address [*ip_address subnet_mask*]
no server ip address

Syntax Description

ip_address	Configures a static IP address for the Cisco E-Series Server.
subnet_mask	The subnet mask associated with the IP address.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

Use this command from interface configuration mode:

```
Router(config)# interface ucse slot/port
```

Examples

The following example shows how to configure a static IP address for the Cisco E-Series Server:

```
Router(config)# interface ucse 2/0
Router(config-if)# server ip address 10.0.0.2 100.1.1.31
```

service alarm persistency interval

To configure alarm history that helps in defining the periodicity or the interval at which the alarm entries are saved in the designated file., use the **service alarm persistency interval** command.

Syntax Description

Syntax Description

service alarm persistency interval *value*	Configures the alarm history helps in defining the periodicity or the interval at which the alarm entries are saved in the designated file. When alarm history is configured, two log files are created in bootflash:tracelogs.

Command Default

This default is 20 seconds.

Command Modes

Global configuration

Command History

Release	Modification
XE 3.18 SP	Support for this command was introduced on NCS 4200 Series.
XE Everest 16.5.1	This command was integrated on the Cisco NCS 4200 Series and Cisco ASR 900 Series Routers.

Examples

The following example shows the configuration of alarm history:

```
enable
configure terminal
service alarm persistency interval 20-600
end
```

Related Commands

Command	Description
show process | include persis	Verifies the validity of the process during alarm history configuration.

service declassify

To enable the declassification function to monitor the auxiliary (AUX) port Clear To Send (CTS) pin, use the **servicedeclassify** command in global configuration mode. To disable, use the **no** form of this command.

service declassify [{**erase-flash** | **erase-nvram** | **erase-all**}]
no service declassify [{**erase-flash** | **erase-nvram** | **erase-all**}]

Syntax Description

erase-flash	(Optional) Erases all files in the Flash memory file system when declassification is invoked.
erase-nvram	(Optional) Erases all files in the NVRAM file system when declassification is invoked.
erase-all	(Optional) Scrubs and erases all files on the router when declassification is invoked.

Note The **servicedeclassify** command is supported on the Cisco 3200 series routers only.

Command Default Zeroization is disabled.

Command Modes Global configuration

Command History

Release	Modification
12.3(8)YD	This command was introduced.
12.4(2)T	This command was integrated into Cisco IOS Release 12.4(2)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The network interfaces are shut down when declassification is invoked.

No command-line interface (CLI) command invokes the declassification process. Declassification is invoked by using an external signal that appears on the AUX port of the router. When declassification is complete, the ROMMON prompt appears on the console.

The output that appears on the console when declassification is initiated depends on what options have been configured. Because of the complex interactions between the declassification process and the logging process during declassification, it is not possible to document exactly what appears on the screen.

Examples

The following example shows the console output when declassification is invoked:

The erase-all Keyword

The output on the console when the **erase-all** keyword is used resembles the following:

```
Router# service declassify erase-all
*Mar  5 17:44:28.347:
Declassification initiated...
*Mar  5 17:44:30.647: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to
administratively down
*Mar  5 17:44:31.647: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to down
System Bootstrap, Version 12.2(1r) [hftseng-MRC_RM 100], DEVELOPMENT SOFTWARE
Copyright (c) 1994-2002 by cisco Systems, Inc.
C3200 platform with 131072 Kbytes of main memory
rommon 1 >
```

Note If the **servicedeclassifyerase-all** command is configured and the Flash file system is erased, error recovery actions must be initiated to load a bootable image on the router. The startup configuration file is also erased; the router boots from the factory default configuration the next time it is booted.

The erase-flash Keyword

The output on the console when the **erase-flash** keyword is used resembles the following:

```
Router# service declassify erase-flash
*Mar  1 00:01:30.091:
Declassification initiated...
*Mar  1 00:01:34.347: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to
administratively down
*Mar  1 00:01:35.371: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to down
System Bootstrap, Version 12.2(1r) [hftseng-MRC_RM 100], DEVELOPMENT SOFTWARE
Copyright (c) 1994-2002 by cisco Systems, Inc.
C3200 platform with 131072 Kbytes of main memory
rommon 1 >
```

Note The Flash file system is erased and there will not be a bootable image for the router in the Flash file system if the **servicedeclassifyerase-flash** command is configured. Error recovery actions must be initiated to load a bootable image. The startup configuration file is not erased if the **servicedeclassifyerase-flash** command is configured. When the router is booted, it is configured using its startup configuration file in NVRAM.

The erase-nvram Keyword

The output on the console when the **erase-nvram** keyword is used resembles the following:

```
Router# service declassify erase-nvram
System Bootstrap, Version 12.2(1r) [hftseng-MRC_RM 100], DEVELOPMENT SOFTWARE
Copyright (c) 1994-2002 by cisco Systems, Inc.
C3200 platform with 131072 Kbytes of main memory
rommon 1 >
```

Note If the **servicedeclassifyerase-nvram** command is configured, the Flash file system is not erased. The bootable image in the Flash file system remains, and the router can be booted. The startup configuration file is erased; because the router has no configuration file, it boots from the default configuration

Related Commands

Command	Description
show declassify	Displays the state of the **servicedeclassify** command.

service-engine default-gateway

To define a default gateway router IP address for the Cisco WebEx Node SPA in a Cisco ASR 1000 Series Router, use the **service-enginedefault-gateway**command in interface configuration mode. To remove the default-gateway IP address, use the **no** form of this command.

service-engine default-gateway *gateway-ip-address*
no service-engine default-gateway *gateway-ip-address*

Syntax Description

gateway-ip-address	IP address of the router default gateway.

Command Default

No gateway IP address is configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
IOS XE Release 2.4	This command was introduced.

Usage Guidelines

The **service-enginedefault-gateway** command specifies the IP address for the default gateway router to be used for the Cisco WebEx Node SPA.

A service-engine interface on the Cisco WebEx Node SPA has two IP addresses:

- Router-side IP address--Configured with the **ipaddress**command. The IP address on the router side acts like a gateway to the WebEx services running on the SPA side. This router-side IP address must match the IP address configured in the **service-enginedefault-gateway** command.
- Internal SPA interface IP address--Configured with the**service-engineipaddress**command.

You must configure the **service-engineipaddress** command before configuring the default gateway.

Note Before you can configure the Cisco WebEx Node SPA, you must shut down the service-engine interface using the **shutdown** interface configuration command. To activate the service-engine interface, use the **noshutdown** command.

Examples

The following example defines the gateway on IP address 10.200.72.17 as the default router for the SPA in slot 1/0/0, which corresponds to the IP address configured on the router side in the**ipaddress**command:

```
Router(config) interface Service-Engine1/0/0
Router(config-if) shutdown
Router(config-if) ip address 10.200.72.17 255.255.255.252
Router(config-if) service-engine ip address 10.200.72.18 255.255.255.252
Router(config-if) service-engine default-gateway 10.200.72.17
```

Related Commands

Command	Description
service-engine hostname	Specifies or modifies the hostname or domain name associated with a Cisco WebEx Node SPA.
service-engine ip address	Selects and configures the internal interface for management traffic on a Cisco WebEx Node SPA.
service-engine nameserver	Specifies the primary and secondary domain name server used by the Cisco WebEx Node SPA.
service-engine wma-passcode	Configures the name and key that are used for authentication on a Cisco WebEx Node SPA.
service-engine wma-token	Configures an encrypted token on a Cisco WebEx Node SPA.
service-engine wma-url	Specifies the URL to which the Cisco WebEx Node SPA must connect to enable WebEx meetings.
show hw-module subslot service-engine status	Displays the Cisco WebEx Node SPA application status.

service-engine hostname

To specify or modify the hostname or domain name associated with a Cisco WebEx Node SPA on a Cisco ASR 1000 Series Router, use the **service-enginehostname**command in interface configuration mode. To remove the hostname and domain name association, use the **no** form of this command.

service-engine hostname *module-side-hostname module-side-domain-name*
no service-engine hostname *module-side-hostname module-side-domain-name*

Syntax Description

module-side-hostname	Name of the hostname associated with a Cisco WebEx Node SPA.
module-side-domain- name	Name of the domain associated with a Cisco WebEx Node SPA

Command Default

No hostname or domain name is configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
IOS XE Release 2.4	This command was introduced.

Usage Guidelines

The **service-enginehostname**command specifies the hostname and domain names given to a Cisco WebEx Node SPA. It is an optional configuration and is only used if a Domain Name System (DNS) entry was created for the IP address assigned to the SPA.

To display the configured hostname and domain name for a Cisco WebEx Node SPA, use the **showhw-modulesubslotservice-enginestatus** command.

Note Before you can configure the Cisco WebEx Node SPA, you must shut down the service-engine interface using the **shutdown** interface configuration command. To activate the service-engine interface, use the **noshutdown** command.

Examples

The following example shows how to specify the hostname and domain name for a Cisco WebEx Node SPA:

```
Router(config)# interface service-engine 1/0
Router(config-if)# shutdown
Router(config-if)# service-engine hostname wma-spa-1 cisco.com
```

Related Commands

Command	Description
service-engine default-gateway	Defines a default gateway router IP address for the Cisco WebEx Node SPA.
service-engine ip address	Selects and configures the internal interface for management traffic on a Cisco WebEx Node SPA.

Command	Description
service-engine hostname	Specifies or modifies the hostname or domain name associated with a Cisco WebEx Node SPA.
service-engine nameserver	Specifies the primary and secondary domain name server used by the Cisco WebEx Node SPA.
service-engine wma-passcode	Configures the name and key that are used for authentication on a Cisco WebEx Node SPA.
service-engine wma-token	Configures an encrypted token on a Cisco WebEx Node SPA.
service-engine wma-url	Specifies the URL to which the Cisco WebEx Node SPA must connect to enable WebEx meetings.
show hw-module subslot service-engine status	Displays the Cisco WebEx Node SPA application status.

service-engine ip address

To select and configure the internal interface for management traffic for the WebEx Node SPA on a Cisco ASR 1000 Series Router, use the **service-engineipaddress**command in interface configuration mode. To delete the IP address associated with this interface, use the **no** form of this command.

service-engine ip address *module-side-ip-address subnet-mask*
no service-engine ip address *module-side-ip-address subnet-mask*

Syntax Description

module-side-ip-address	Specifies the IP address of the internal network module-side interface.
subnet-mask	Specifies the subnet mask to append to the IP address.

Command Default

No IP address is configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
IOS XE Release 2.4	This command was introduced.

Usage Guidelines

A service-engine interface on the Cisco WebEx Node SPA has two IP addresses:

- Router-side IP address--Configured with the **ipaddress**command. The IP address on the router side acts like a gateway to the WebEx services running on the SPA side. This router-side IP address must match the IP address configured in the **service-enginedefault-gateway** command.
- Internal SPA interface IP address--Configured with the**service-engineipaddress**command.

To successfully configure the service-engine IP address, consider the following guidelines:

- The router-side IP address must be configured using the **ipaddress** command.
- The service-engine IP address must be on the same subnet as the router-side IP address for the service-engine interface (configured using the **ipaddress**command.)
- The **service-engineipaddress**command must be configured before you configure the **service-enginedefault-gateway** command.

Note Before you can configure the Cisco WebEx Node SPA, you must shut down the service-engine interface using the **shutdown** interface configuration command. To activate the service-engine interface, use the **noshutdown** command.

Examples

The following example shows how to define an IP address for the internal SPA-side interface on the WebEx Node SPA in slot 1 using the **service-engineipaddress**command. The example shows the service-engine IP address on the same subnet as the router-side IP address that is configured with the **ipaddress** command:

```
Router(config) interface Service-Engine1/0/0
Router(config-if) shutdown
Router(config-if) ip address 10.200.72.17 255.255.255.252
Router(config-if) service-engine ip address 10.200.72.18 255.255.255.252
Router(config-if) service-engine default-gateway 10.200.72.17
```

Related Commands

Command	Description
service-engine default-gateway	Defines a default gateway router IP address for the Cisco WebEx Node SPA.
service-engine hostname	Specifies or modifies the hostname or domain name associated with a Cisco WebEx Node SPA.
service-engine nameserver	Specifies the primary and secondary domain name server used by the Cisco WebEx Node SPA.
service-engine wma-passcode	Configures the name and key that are used for authentication on a Cisco WebEx Node SPA.
service-engine wma-token	Configures an encrypted token on a Cisco WebEx Node SPA.
service-engine wma-url	Specifies the URL to which the Cisco WebEx Node SPA must connect to enable WebEx meetings.
show hw-module subslot service-engine status	Displays the Cisco WebEx Node SPA application status.

service-engine nameserver

To specify the primary and secondary Domain Name System (DNS) used by the Cisco WebEx Node SPA in a Cisco ASR 1000 Series Router, use the **service-enginenameserver**command in interface configuration mode. To remove a DNS name server from the list, use the **no** form of this command.

service-engine nameserver *name-server1-ip-address name-server2-ip-address*
no service-engine nameserver *name-server1-ip-address name-server2-ip-address*

Syntax Description

name-server1-ip- address	IP address of the primary DNS name server for the WebEx Node SPA.
name-server2-ip- address	IP address of a secondary DNS name server for the WebEx Node SPA.

Command Default

No name servers are configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
IOS XE Release 2.4	This command was introduced.

Usage Guidelines

Note Before you can configure the Cisco WebEx Node SPA, you must shut down the service-engine interface using the **shutdown** interface configuration command. To activate the service-engine interface, use the **noshutdown** command.

Examples

The following example shows how to specify the hosts at 192.168.2.111 and 192.168.2.112 as the primary and secondary name servers for the WebEx Node SPA in slot 1/0:

```
Router(config)# interface service-engine 1/0
Router(config-if)# shutdown
Router(config-if)# service-engine nameserver 192.168.2.111
 192.168.2.112
```

Related Commands

Command	Description
service-engine default-gateway	Defines a default gateway router IP address for the Cisco WebEx Node SPA.
service-engine hostname	Specifies or modifies the hostname or domain name associated with a Cisco WebEx Node SPA.
service-engine ip address	Selects and configures the internal interface for management traffic on a Cisco WebEx Node SPA.

Command	Description
service-engine wma-passcode	Configures the name and key that are used for authentication on a Cisco WebEx Node SPA.
service-engine wma-token	Configures an encrypted token on a Cisco WebEx Node SPA.
service-engine wma-url	Specifies the URL to which the Cisco WebEx Node SPA must connect to enable WebEx meetings.
show hw-module subslot service-engine status	Displays the Cisco WebEx Node SPA application status.

service-engine wma-passcode

To configure the name and key that is used for authentication for a Cisco WebEx Node SPA in a Cisco ASR 1000 Series Router, use the **service-enginewma-passcode** command in interface configuration mode. To disable this function, use the **no** form of this command.

service-engine wma-passcode *name-string key-string*
no service-engine wma-passcode

Syntax Description

name-string	Specifies the authentication name for the WebEx Node SPA.
key-string	Specifies the authentication passcode for the WebEx Node SPA.

Command Default

The name and key used for authentication for a Cisco WebEx Node SPA is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
IOS XE Release 2.4	This command was introduced.

Usage Guidelines

The **service-enginewma-passcode**command is used to configure the Cisco WebEx Node SPA name and passcode key to identify the node. Both the passcode and the token (configured using the **service-enginewma-token** command) are used together for authentication of the Cisco WebEx Node SPA.

Before you can configure this command, you must first provision the Cisco WebEx Node SPA at the WebEx Data Center. The value of the passcode string provisioned in the Cisco WebEx Node Management System for the SPA must match the value of the passcode string configured in the **service-enginewma-passcode**command. For more information, refer to the “Configuring the Cisco WebEx Node for ASR 1000 Series” chapter of the Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Software Configuration Guide .

Note Before you can configure the Cisco WebEx Node SPA, you must shut down the service-engine interface using the **shutdown** interface configuration command. To activate the service-engine interface, use the **noshutdown** command.

Once you configure the **service-enginewma-passcode** command and enter the *key-string* into the running configuration, the *key-string* is encrypted. Therefore, you cannot successfully copy the passcode from the running configuration or a backup version of your configuration file to running-configuration. The **service-enginewma-passcode** command must be re-entered.

Examples

The following example defines the authentication SPA name and passcode for the Cisco WebEx Node SPA in slot 1/0:

```
Router(config)# interface service-engine 1/0
Router(config-if)# shutdown
Router(config-if)# service-engine wma-passcode wma-spa-1 spa1pass
```

Related Commands

Command	Description
service-engine default-gateway	Defines a default gateway router IP address for the Cisco WebEx Node SPA.
service-engine ip address	Selects and configures the internal interface for management traffic on a Cisco WebEx Node SPA.
service-engine hostname	Specifies or modifies the hostname or domain name associated with a Cisco WebEx Node SPA.
service-engine nameserver	Specifies the primary and secondary domain name server used by the Cisco WebEx Node SPA.
service-engine wma-token	Configures an encrypted token on a Cisco WebEx Node SPA.
service-engine wma-url	Specifies the URL to which the Cisco WebEx Node SPA must connect to enable WebEx meetings.
show hw-module subslot service-engine status	Displays the Cisco WebEx Node SPA application status.

service-engine wma-token

To configure an encrypted token for a Cisco WebEx Node SPA in a Cisco ASR 1000 Series Router, use the **service-enginewma-token**command in interface configuration mode. To disable this function, use the **no** form of this command.

service-engine wma-token *token-string*
no service-engine wma-token

Syntax Description

token-string	Specifies the encrypted token for the WebEx Node SPA.

Command Default

The encrypted token for a Cisco WebEx Node SPA is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
IOS XE Release 2.4	This command was introduced.

Usage Guidelines

The **service-enginewma-token**command is used to configure an encrypted token for the Cisco WebEx Node SPA. Both the token and the passcode (configured using the **service-enginewma-passcode**command) are used together for authentication of the Cisco WebEx Node SPA.

Before you can configure this command, you must first provision the Cisco WebEx Node SPA at the WebEx Data Center. The value of the token string provisioned in the Cisco WebEx Node Management System for the SPA must match the value of the passcode string configured in the **service-enginewma-token**command. For more information, refer to the “Configuring the Cisco WebEx Node for ASR 1000 Series” chapter of the Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Software Configuration Guide .

Note Before you can configure the Cisco WebEx Node SPA, you must shut down the service-engine interface using the **shutdown** interface configuration command. To activate the service-engine interface, use the **noshutdown**command.

Examples

The following example specifies the token for the Cisco WebEx Node SPA in slot 1/0:

```
Router(config)# interface service-engine 1/0
Router(config-if)# shutdown
Router(config-if)# service-engine wma-token 123456789
```

Related Commands

Command	Description
service-engine default-gateway	Defines a default gateway router IP address for the Cisco WebEx Node SPA.
service-engine ip address	Selects and configures the internal interface for management traffic on a Cisco WebEx Node SPA.

Command	Description
service-engine hostname	Specifies or modifies the hostname or domain name associated with a Cisco WebEx Node SPA.
service-engine nameserver	Specifies the primary and secondary domain name server used by the Cisco WebEx Node SPA.
service-engine wma-passcode	Configures the name and key that are used for authentication on a Cisco WebEx Node SPA.
service-engine wma-url	Specifies the URL to which the Cisco WebEx Node SPA must connect to enable WebEx meetings.
show hw-module subslot service-engine status	Displays the Cisco WebEx Node SPA application status.

service-engine wma-url

To specify the URL to which the Cisco WebEx Node SPA in a Cisco ASR 1000 Series Router must connect to enable WebEx meetings, use the **service-enginewma-url**command in interface configuration mode. To disable this function, use the **no** form of this command.

service-engine wma-url *url-string*
no service-engine wma-url

Syntax Description

url-string	Specifies the URL to connect to the WebEx MediaTone Center.

Command Default

No URL string is configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
IOS XE Release 2.4	This command was introduced.

Usage Guidelines

The**service-enginewma-url** command is used to configure the URL that enables connectivity to the WebEx Data Center.

Before you can configure this command, you must first provision the Cisco WebEx Node SPA at the WebEx Data Center. The URL string provisioned in the Cisco WebEx Node Management System for the SPA must match the value of the URL configured in the **service-enginewma-url**command. For more information, refer to the "Configuring the Cisco WebEx Node for ASR 1000 Series" chapter of the Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Software Configuration Guide .

Note Before you can configure the Cisco WebEx Node SPA, you must shut down the service-engine interface using the **shutdown** interface configuration command. To activate the service-engine interface, use the **noshutdown** command.

Examples

The following example specifies the URL to which the Cisco WebEx Node SPA in slot 1/0 must connect:

```
Router(config)# interface service-engine 1/0
Router(config-if)# shutdown
Router(config-if)# service-engine wma-url https://spa.webex.com
```

Related Commands

Command	Description
service-engine default-gateway	Defines a default gateway router IP address for the Cisco WebEx Node SPA.
service-engine ip address	Selects and configures the internal interface for management traffic on a Cisco WebEx Node SPA.

Command	Description
service-engine hostname	Specifies or modifies the hostname or domain name associated with a Cisco WebEx Node SPA.
service-engine nameserver	Specifies the primary and secondary domain name server used by the Cisco WebEx Node SPA.
service-engine wma-passcode	Configures the name and key that are used for authentication on a Cisco WebEx Node SPA.
service-engine wma-token	Configures an encrypted token on a Cisco WebEx Node SPA.
show hw-module subslot service-engine status	Displays the Cisco WebEx Node SPA application status.

service single-slot-reload-enable

To enable single line card reloading for all line cards in the Cisco 7500 series router, use the **servicesingle-slot-reload-enable**command in global configuration mode. To disable single line card reloading for the line cards in the Cisco 7500 series router, use the **no** form of this command.

service single-slot-reload-enable
no service single-slot-reload-enable

Syntax Description

This command has no arguments or keywords.

Command Default

Single line card reloading is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(13)S	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

In the following example, single line card reloading is enabled for all lines cards on the Cisco 7500 series router:

```
Router(config)# service single-slot-reload-enable
```

Related Commands

Command	Description
show diag	Displays hardware information for a networking device.
show running-config	Displays configuration information.

service-module

To set service module parameters, use the **service-module**commandinprivilegedEXEC mode.

service-module GigabitEthernet *interface-number* {**heartbeat-reset** {**disable** | **enable**} | **password-reset** | **reload** | **reset** | **session** [**clear**] | **shutdown** [**no-confirm**] | **statistics** [**clear**] | **status**}

Syntax Description

GigabitEthernet *interface-number*	Specifies the Gigabit Ethernet interface number.
heartbeat-reset	Specifies the heartbeat failure to reset the service module.
disable	Disables the heartbeat reset.
enable	Enables the heartbeat reset.
password-reset	Specifies the password reset for the service module.
reload	Reloads the service module.
reset	Resets the service module hardware.
session	Specifies the service module session.
clear	(Optional) Clears the existing service module session when used with the **session** keyword. Clears the service module statistics when used with the **statistics** keyword.
shutdown	Shuts down the service module.
no-confirm	(Optional) Configures the system not to confirm before the shutdown.
statistics	Specifies service module statistics.
status	Specifies service module status information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use this command with the **reset** keyword only to recover from the shutdown or failed state. Use the **shutdown** keyword for online removal of a service module. When you shut down a service module on switch modules, the line protocol on the GigabitEthernet interface goes down. If the line protocol does not go down, first shut down the interface using the **shutdown** command in interface configuration mode and then shut down the service module using the **service-moduleGigabitEthernet***interface-number***shutdown** command.

Examples

The following example shows how to disable the heartbeat reset:

```
Router# service-module GigabitEthernet 1/0 heartbeat-reset disable
```

The following example shows the status of the service module:

Router# **service-moduleGigabitEthernet1/0status**

```
Service Module is Cisco GigabitEthernet1/0
Service Module supports session via TTY line 66
Service Module is Shutdown
Service Module reset on error is disabled
Service Module heartbeat-reset is enabled
Service Module status is not available
```

The following example shows how to shut down an interface before shutting down the service module:

```
Router(config)# interface GigabitEthernet 1/0
Router(config-if)# shutdown
```

The following example shows how to shut down a service module:

```
Router# service-module GigabitEthernet 1/0 shutdown
```

Related Commands

Command	Description
show interfaces sm	Displays basic interface configuration information for service modules.
shutdown (interface)	Disables an interface.

service-module 56k clock rate

To configure the network line speed for a serial interface on a 4-wire, 56/64-kbps CSU/DSU module, use the **service-module56kclockrate**command in interface configuration mode. To enable a network line speed of 56 kbps, which is the default, use the **no** form of this command.

service-module 56k clock rate commandservice-module 56k clock rate *speed*
no service-module 56k clock rate *speed*

Syntax Description

speed	Network line speed in kbps. The default speed is 56 kbps. Choose from one of the following optional speeds: • **2.4** -- 2.4 kbps • **4.8** -- 4.8 kbps • **9.6** -- 9.6 kbps • **19.2** -- 19.2 kbps • **38.4** -- 38.4 kbps • **56** -- 56 kbps (default) • **64** -- 64 kbps • **auto** --Automatic line speed mode. Configure this option if your line speed is constantly changing.

Command Default

56 kbps

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The 56-kbps line speed is available in switched mode, which is enabled using the **service-module56knetwork-type** interface configuration command on the 4-wire CSU/DSU. If you have a 2-wire CSU/DSU module, the default is automatically set to switched mode.

The 64-kbps line speed cannot be used with back-to-back digital data service (DDS) lines. The subrate line speeds are determined by the service provider.

The **auto**keyword enables the CSU/DSU to decipher current line speed from the sealing current running on the network. Use the **auto** keyword only when transmitting over telco DDS lines and the clocking source is taken from the line.

Examples

The following example displays two routers connected in back-to-back DDS mode. However, notice that at first the configuration fails because the **auto** option is used. Later in the example the correct matching configuration is issued, which is 38.4 kbps.

```
Router1(config)# interface serial 0
Router1(config-if)# service-module 56k clock source internal
Router1(config-if)# service-module 56k clock rate 38.4
Router2(config-if)# service-module 56k clock rate auto
Router1# ping 10.1.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Router2(config-if)# service-module 56k clock rate 38.4

Router1# ping 10.1.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/54/56 ms
```

When transferring from DDS mode to switched mode, you must set the correct clock rate, as shown in the following example:

```
Router2(config-if)# service-module 56k network-type dds
Router2(config-if)# service-module 56k clock rate 38.4
Router2(config-if)# service-module 56k network-type switched
% Have to use 56k or auto clock rate for switched mode
% Service module configuration command failed: WRONG FORMAT.
Router2(config-if)# service-module 56k clock rate auto
% WARNING - auto rate will not work in back-to-back DDS.
Router2(config-if)# service-module 56k network-type switched
```

Related Commands

Command	Description
service-module 56k clock source	Sets up the clock source on a serial interface for a 4-wire, 56/64-kbps CSU/DSU module.
service-module 56k network-type	Sends packets in switched dial-up mode or DDS mode using a serial interface on a 4-wire, 56/64-kbps CSU/DSU module.

service-module 56k clock source

To set up the clock source on a serial interface for a 4-wire, 56/64-kbps CSU/DSU module, use the **service-module56kclocksource**command in interface configuration mode. To specify that the clocking come from the line, use the **no** form of this command.

service-module 56k clock source commandservice-module 56k clock source {**line** | **internal**}
no service-module 56k clock source {**line** | **internal**}

Syntax Description

line	Uses the clocking provided by the active line coming in to the router. This is the default.
internal	Uses the internal clocking provided by the hardware module.

Command Default

Line clock

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

In most applications, the CSU/DSU should be configured with the **clocksourceline** command. For back-to-back configurations, configure one CSU/DSU with the **clocksourceinternal** command and the other with **clocksourceline** command.

Examples

The following example configures internal clocking and transmission speed at 38.4 kbps.

```
Router(config)# interface serial 0
Router(config-if)# service-module 56k clock source internal
Router(config-if)# service-module 56k clock rate 38.4
```

Related Commands

Command	Description
clock source (interface)	Controls the clock used by a G.703-E1 interface.
service-module 56k clock rate	Configures the network line speed for a serial interface on a 4-wire, 56/64-kbps CSU/DSU module.

service-module 56k data-coding

To prevent application data from replicating loopback codes when operating at 64 kbps on a 4-wire CSU/DSU, use the **service-module56kdata-coding** command in interface configuration mode. To enable normal transmission, use the **no** form of this command.

service-module 56k data-coding {**normal** | **scrambled**}
no service-module 56k data-coding {**normal** | **scrambled**}

Syntax Description

normal	Specifies normal transmission of data. This is the default.
scrambled	Scrambles bit codes or user data before transmission. All control codes such as out-of-service and out-of-frame are avoided.

Command Default

Normal data transmission

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Enable the scrambled configuration only in 64-kbps digital data service (DDS) mode. If the network type is set to switched, the configuration is refused.

If you transmit scrambled bit codes, both CSU/DSUs must have this command configured for successful communication.

Examples

The following example s crambles bit codes or user data before transmission :

```
Router(config)# interface serial 0
Router(config-if)# service-module 56k clock rate 64
Router(config-if)# service-module 56k data-coding scrambled
```

Related Commands

Command	Description
service-module 56k clock rate	Configures the network line speed for a serial interface on a 4-wire, 56/64-kbps CSU/DSU module.

service-module 56k network-type

To transmit packets in switched dial-up mode or digital data service (DDS) mode using a serial interface on a 4-wire, 56/64-kbps CSU/DSU module, use the **service-module56knetwork-type**command in interface configuration mode. To transmit from a dedicated leased line in DDS mode, use the **no** form of this command.

service-module 56k network-type {**dds** | **switched**}
no service-module 56k network-type {**dds** | **switched**}

Syntax Description

dds	Transmits packets in DDS mode or through a dedicated leased line. The default is DDS enabled for the 4-wire CSU/DSU.
switched	Transmits packets in switched dial-up mode. On a 2-wire, switched 56-kbps CSU/DSU module, this is the default and only setting.

Command Default

DDS is enabled for the 4-wire CSU/DSU. Switched is enabled for the 2-wire CSU/DSU.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

In switched mode, you need additional dialer configuration commands to configure dial-out numbers. Before you enable the **service-module56knetwork-typeswitched** command, both CSU/DSUs must use a clock source coming from the line and have the clock rate configured to **auto** or **56** kbps. If the clock rate is not set correctly, this command will not be accepted.

The 2-wire and 4-wire, 56/64-kbps CSU/DSU modules use V.25 *bis* dial commands to interface with the router. Therefore, the interface must be configured using the**dialerin-band** command. Data terminal ready (DTR) dial is not supported.

Note Any loopbacks in progress are terminated when switching between modes.

Examples

The following example configures transmission in switched dial-up mode :

```
Router(config)# interface serial 0
Router(config
-if)#
 service-module 56k clock rate auto
Router(config
-if)#
```

```
 service-module 56k network-type switched
Router(config
-if)#
 dialer in-band
Router(config
-if)#
 dialer string 5550111
Router(config
-if)#
 dialer-group 1
```

Related Commands

Command	Description
dialer in-band	Specifies that DDR is to be supported.
service-module 56k clock rate	Configures the network line speed for a serial interface on a 4-wire, 56/64-kbps CSU/DSU module.
service-module 56k clock source	Sets up the clock source on a serial interface for a 4-wire, 56/64-kbps CSU/DSU module.
service-module 56k switched-carrier	Selects a service provider to use with a 2- or 4-wire, 56/64-kbps dial-up serial line.

service-module 56k remote-loopback

To enable the acceptance of a remote loopback request on a serial interface on a 2- or 4-wire, 56/64-kbps CSU/DSU module, use the **service-module56kremote-loopback** command in interface configuration mode. To disable the module from entering loopback, use the **no** form of this command.

service-module 56k remote-loopback commandservice-module 56k remote-loopback
no service-module 56k remote-loopback commandservice-module 56k remote-loopback

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **noservice-module56kremote-loopback** command prevents the local CSU/DSU from being placed into loopback by remote devices on the line. The line provider is still able to put the module into loopback by reversing sealing current. Unlike the T1 module, the 2- or 4-wire, 56/64-kbps CSU/DSU module can still initiate remote loopbacks with the **no** form of this command configured.

Examples

The following example enables transmitting and receiving remote loopbacks:

```
Router(config)# interface serial 0
Router(config
-if)
# service-module 56k remote-loopback
```

Related Commands

Command	Description
loopback remote (interface)	Loops packets through a CSU/DSU, over a DS3 link or a channelized T1 link, to the remote CSU/DSU and back.

service-module 56k switched-carrier

To select a service provider to use with a 2- or 4-wire, 56/64-kbps dial-up serial line, use the **service-module56kswitched-carrier** command in interface configuration mode. To enable the default service provider, use the **no** form of this command.

service-module 56k switched-carrier {**att** | **sprint** | **other**}
no service-module 56k switched-carrier {**att** | **sprint** | **other**}

Syntax Description

att	AT&T or other digital network service provider. This is the default on the 4-wire, 56/64-kbps CSU/DSU module.
sprint	Sprint or other service provider whose network requires echo cancelers. This is the default on the 2-wire, switched 56-kbps CSU/DSU module.
other	Any other service provider.

Command Default

ATT is enabled on the 4-wire, 56/64-kbps CSU/DSU module. Sprint is enabled on the 2-wire, switched 56-kbps CSU/DSU module.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

On a Sprint network, echo-canceler tones are sent during call setup to prevent the echo cancelers from damaging digital data. The transmission of echo-canceler tones may increase call setup times by 8 seconds on the 4-wire module. Having echo cancellation enabled does not affect data traffic.

This configuration command is ignored if the network type is DDS.

Examples

The following example configures AT&T as a service provider :

```
Router(config)# interface serial 0
Router(config
-if)
# service-module 56k network-type switched
Router(config
-if)
# service-module 56k switched-carrier att
```

Related Commands

Command	Description
service-module 56k network-type	Sends packets in switched dial-up mode or DDS mode using a serial interface on a 4-wire, 56/64-kbps CSU/DSU module.

service-module analysis-module reload

To perform a graceful halt and reboot of the Network Analysis Module (NAM) software on the NM-NAM network module, use the **service-moduleanalysis-modulereload** command in privileged EXEC mode.

service-module **analysis-module** *slot/unit* **reload**

Syntax Description

slot	Number of the router chassis slot for the network module.
/ *unit*	Number of the daughter card on the network module. For the NM-NAM, always use 0. The slash mark is required between the *slot* argument and the *unit*argument.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)XD	This command was introduced on the following platforms: Cisco 2600XM series, Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.3(8)T4	This command was implemented on the following platforms: Cisco 2811, Cisco 2821, and Cisco 2851.
12.3(11)T	This command was implemented on the Cisco 3800 series.

Usage Guidelines

The **service-moduleanalysis-modulereload**command is the Cisco IOS equivalent of the **reboot** NAM CLI command. These commands can be used to initiate the NAM software upgrade process or to access the NAM helper image.

Examples

The following example shows how to gracefully halt and reboot the NAM application software:

```
Router# service-module analysis-module 1/0 reload

Do you want to proceed with reload?[confirm]
Trying to reload Service Module Analysis-Module1/0.
```

Related Commands

Command	Description
service-module analysis-module reset	Resets the hardware on the NM-NAM.
service-module analysis-module shutdown	Gracefully halts the operating system on the NM-NAM.
service-module analysis-module status	Displays hardware and software status information about the NM-NAM.

service-module analysis-module reset

To reset the hardware on the Network Analysis Module (NM-NAM), use the **service-moduleanalysis-modulereset** command in privileged EXEC mode.

service-module analysis-module *slot/unit* **reset**

Syntax Description

slot	Number of the router chassis slot for the network module.
/ *unit*	Number of the daughter card on the network module. For the NM-NAM, always use 0. The slash mark is required between the *slot* argument and the *unit*argument.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)XD	This command was introduced on the following platforms: Cisco 2600XM series, Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.3(8)T4	This command was implemented on the following platforms: Cisco 2811, Cisco 2821, and Cisco 2851.
12.3(11)T	This command was implemented on the Cisco 3800 series.

Usage Guidelines

Use the **service-moduleanalysis-modulereset** command to bring up the NM-NAM after it has been shut down using the **service-moduleanalysis-moduleshutdown** command.

Examples

The following example shows how to reset the hardware on the NM-NAM:

```
Router# service-module analysis-module 1/0 reset

Use reset only to recover from shutdown or failed state
Warning:May lose data on the hard disc!
Do you want to reset?[confirm]
Trying to reset Service Module Analysis-Module1/0.
```

Related Commands

Command	Description
service-module analysis-module reload	Gracefully halts and reboots the software on the NM-NAM.
service-module analysis-module shutdown	Gracefully halts the operating system on the NM-NAM.
service-module analysis-module status	Displays hardware and software status information about the NM-NAM.

service-module analysis-module session

To access the Network Analysis Module (NAM) console from the router, use the **service-moduleanalysis-modulesession** command in privileged EXEC mode.

service-module analysis-module *slot/unit* **session** [**clear**]

Syntax Description

slot	Number of the router chassis slot for the network module.
/ *unit*	Number of the daughter card on the network module. For the NM-NAM, always use 0. The slash mark is required between the *slot* argument and the *unit*argument.
clear	(Optional) Clears the NAM console line.

Command Default

The router cannot access the NAM console.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)XD	This command was introduced on the following platforms: Cisco 2600XM series, Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.3(8)T4	This command was implemented on the following platforms: Cisco 2811, Cisco 2821, and Cisco 2851.
12.3(11)T	This command was implemented on the Cisco 3800 series.

Usage Guidelines

When entered without the **clear** keyword, this command opens a NAM console session from the router.

Examples

Opening a NAM console Session

The following example shows how to open a NAM console session when the NM-NAM is installed in router slot 2:

```
Router# service-module analysis-module 2/0 session

Trying 10.1.1.1, 2065 ... Open
<Press Return>

Cisco Network Analysis Module (NM-NAM)
nam1.cisco.com login: root

Password: <password>

Terminal type: vt100
Cisco Network Analysis Module (NM-NAM) Console, 3.2(0.9)
Copyright (c) 1999-2003 by Cisco Systems, Inc.
```

```
WARNING! Default password has not been changed!
root@nam1.cisco.com#
```

Clearing the NAM Console Line

The following example shows how to clear the NAM console line when the NM-NAM is installed in router slot 1:

```
Router# service-module analysis-module 1/0 session clear

[confirm]
 [OK]
```

Related Commands

Command	Description
ssh	Starts an encrypted session with a remote networking device.
telnet	Logs in to a host that supports Telnet.

service-module analysis-module shutdown

To gracefully halt the operating system on the Network Analysis Module (NM-NAM), use the **service-moduleanalysis-moduleshutdown** command in privileged EXEC mode.

service-module analysis-module *slot/unit* **shutdown** [**no-confirm**]

Syntax Description

slot	Number of the router chassis slot for the network module.
/ *unit*	Number of the daughter card on the network module. For the NM-NAM, always use 0. The slash mark is required between the *slot* argument and the *unit*argument.
no-confirm	(Optional) No confirmation message appears before shutdown.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)XD	This command was introduced on the following platforms: Cisco 2600XM series, Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.3(8)T4	This command was implemented on the following platforms: Cisco 2811, Cisco 2821, and Cisco 2851.
12.3(11)T	This command was implemented on the Cisco 3800 series.

Usage Guidelines

The **service-moduleanalysis-moduleshutdown** command properly brings down the operating system of the Network Analysis Module (NM-NAM) to protect the network module's hard drive. When the operating system has been shut down, the NM-NAM can be removed from the router.

At the confirmation prompt, press **Enter** to confirm the action or **n** to cancel.

If you enter the **no-confirm** keyword, the confirmation prompt does not appear.

Examples

Gracefully Halt the Operating System with Confirmation

The following example shows how to gracefully halt the operating system of the NM-NAM in slot 1:

```
Router# service-module analysis-module 1/0 shutdown

Shutdown is used for Online removal of Service Module.
Do you want to proceed with shutdown?[confirm]
Use service module reset command to recover from shutdown.
```

Gracefully Halt the Operating System -- No Confirmation

The following example shows how to gracefully halt the operating system of the NM-NAM in slot 2 without any user confirmation:

```
Router# service-module analysis-module 2/0 shutdown no-confirm
Use service module reset command to recover from shutdown.
```

Related Commands

Command	Description
service-module analysis-module reload	Gracefully halts and reboots the software on the NM-NAM.
service-module analysis-module reset	Resets the hardware on the NM-NAM.
service-module analysis-module status	Displays hardware and software status information about the NM-NAM.

service-module analysis-module status

To display hardware and software status information about the Network Analysis Module (NM-NAM), use the **service-moduleanalysis-modulestatus** command in privileged EXEC mode.

service-module analysis-module *slot/unit* **status**

Syntax Description

slot	Number of the router chassis slot for the network module.
/ *unit*	Number of the daughter card on the network module. For the NM-NAM, always use 0. The slash mark is required between the *slot* argument and the *unit*argument.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)XD	This command was introduced on the following platforms: Cisco 2600XM series, Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.3(8)T4	This command was implemented on the following platforms: Cisco 2811, Cisco 2821, and Cisco 2851.
12.3(11)T	This command was implemented on the Cisco 3800 series.

Usage Guidelines

Use the **service-moduleanalysis-modulestatus** command to:

- Display the NAM software release version.
- Check the NAM status (steady or down).

Examples

The command in the following example displays information about the NM-NAM in router slot 1:

```
Router# service-module analysis-module 1/0 status

Service Module is Cisco Analysis-Module1/0
Service Module supports session via TTY line 33
Service Module is in Steady state
Getting status from the Service Module, please wait...
Cisco Network Analysis Module (NM-NAM), version 3.2(0.8)
```

Related Commands

Command	Description
show controllers analysis-module	Displays controller information for the analysis module interface.
show interfaces analysis-module	Displays status, traffic data, and configuration information about the analysis module interface.

service-module backup interface

To configure an interface as a secondary or dial backup to the satellite interface, use the **servicemodulebackupinterface** command in satellite interface configuration mode. To remove the backup interface configuration, use the **no** form of this command.

service module backup interface *interface*
no service module backup interface *interface*

Syntax Description

interface	Interface type and number.

Command Default

No default behavior or values

Command Modes

Satellite interface configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Examples

The following example shows how to set interface async 1 as the backup to the satellite link:

```
Router(config-if)# service-module backup interface async1
```

Related Commands

Command	Description
service-module backup mode	Sets the terrestrial backup mode for the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT).

service-module backup mode

To set the terrestrial dial backup mode for the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT), use the **service-modulebackupmode** command in satellite interface configuration mode. To return to the router (default) dial backup mode, use the **no** form of this command.

service-module backup mode [{**hub** | **router**}]
no service-module backup mode

Syntax Description

hub	Hub dial backup mode.
router	Router dial backup mode.

Command Default

Router dial backup mode

Command Modes

Satellite interface configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Hub Dial Backup Mode

Hub dial backup mode maintains TCP connections during transitions between primary and backup links. Note, however, that hub dial backup mode provides backup for the satellite *link* , but not for the NM-1VSAT-GILAT network module hardware, the router satellite interface, or other router interfaces. If the satellite link goes down (for example, because of rain fade) in hub dial backup mode, the NM-1VSAT-GILAT network module connects to the hub using dial-on-demand routing (DDR). Common DDR backup links use ISDN BRIs, modems on auxiliary ports, and T1/E1 lines.

The NM-1VSAT-GILAT network module always encapsulates packets using a satellite backbone protocol before sending the packets over the satellite link. In hub dial backup mode, the NM-1VSAT-GILAT network module continues to encapsulate the packets using the satellite backbone protocol before sending the packets over the dial backup link to the hub; this is how hub dial backup mode maintains TCP connections during transitions between the primary satellite link and the dial backup link. Therefore, hub dial backup mode works only when the NM-1VSAT-GILAT network module itself is functioning properly.

Router Dial Backup Mode

If the satellite link goes down in router dial backup mode, the router uses DDR to send data out a different interface. Unlike hub dial backup mode, router dial backup mode does these things:

- Tears down and reestablishes TCP connections during transitions between primary and backup links
- Does not require that the NM-1VSAT-GILAT network module work properly while the backup link is in use

Examples

The following example shows how to specify hub backup mode:

```
Router(config-if)# service-module backup mode hub
```

The following example shows how to specify router backup mode:

```
Router(config-if)# service-module backup mode router
```

Related Commands

Command	Description
service-module backup interface	Specifies the interface to use to back up the satellite interface.

service-module content-engine reload

To perform a graceful halt and reboot of a content engine (CE) network module operating system, use the **service-modulecontent-enginereload** command in privileged EXEC mode.

service-module content-engine *slot/unit* **reload**

Syntax Description

slot	Number of the router chassis slot for the network module.
/ *unit*	Number of the daughter card on the network module. For CE network modules, always use 0. The slash mark is required between the *slot* argument and the *unit*argument.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)YT	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

At the confirmation prompt, press **Enter** to confirm the action or **n** to cancel.

Examples

The following example gracefully halts and reboots the CE network module operating system in slot 1:

```
Router# service-module content-engine 1/0 reload
Do you want to proceed with reload?[confirm]
```

Related Commands

Command	Description
interface content-engine	Configures an interface for a CE network module and enters interface configuration mode.
service-module content-engine reset	Resets the hardware on a CE network module.
service-module content-engine shutdown	Gracefully halts a CE network module.
show controllers content-engine	Displays controller information for CE network modules.
show interfaces content-engine	Displays basic interface configuration information for a CE network module.

service-module content-engine reset

To reset the hardware on a content engine (CE) network module, use the **service-modulecontent-enginereset** command in privileged EXEC mode.

service-module content-engine *slot/unit* **reset**

Syntax Description

slot	Number of the router chassis slot for the network module.
/ *unit*	Number of the daughter card on the network module. For CE network modules, always use 0. The slash mark is required between the *slot* argument and the *unit*argument.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)YT	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

At the confirmation prompt, press **Enter** to confirm the action or **n** to cancel.

Note Use the **service-modulecontent-enginereset** command only to recover from a shutdown or failed state because you may lose data.

Examples

The following example resets the hardware on the CE network module in slot 1:

```
Router# service-module content-engine 1/0 reset
Use reset only to recover from shutdown or failed state
Warning: May lose data on the hard disc!
Do you want to reset?[confirm]
```

Related Commands

Command	Description
interface content-engine	Configures an interface for a CE network module and enters interface configuration mode.
service-module content-engine reload	Performs a graceful halt and reboot of a CE network module operating system.
service-module content-engine shutdown	Gracefully halts a CE network module.
show controllers content-engine	Displays controller information for CE network modules.
show interfaces content-engine	Displays basic interface configuration information for a CE network module.

service-module content-engine session

To access a content engine (CE) network module console and begin a configuration session, use the **service-modulecontent-enginesession** command in privileged EXEC mode.

service-module content-engine *slot* / *unit* **session** [**clear**]

Syntax Description

slot	Number of the router chassis slot for the network module.
/ *unit*	Number of the daughter card on the network module. For CE network modules, always use 0. The slash mark is required between the *slot* argument and the *unit*argument.
clear	(Optional) Clears the CE configuration session.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)YT	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

Only one session at a time is allowed into the content engine from the internal CE network-module-side interface. This interface provides console access to the CE network module from the router command-line interface (CLI) by initiating a reverse Telnet connection that uses the IP address of the CE interface and the terminal (TTY) line associated with the CE network module. The TTY line number is calculated using the formula (n*32) + 1, where *n* is the number of the chassis slot that contains the CE network module. The CE interface must be up before you can use this command.

Once a session is started, you can perform any CE configuration task. You first access the CE console in a user-level shell. To access the privileged EXEC command shell, where most commands are available, use the **enable** command. Note that this is a Cisco Application and Content Networking System (ACNS) software command, not a Cisco IOS software command.

CE configuration tasks are described in the documentation for Cisco Application and Content Networking Software, *Release 4.2. Initial CE configuration tasks are covered in the* Cisco Content Delivery Networking Products Getting Started Guide, *section 6, "Perform an Initial Startup Configuration."*

After you finish CE configuration and exit the CE console session, use this command with the **clear** keyword to clear the session. At the confirmation prompt, press **Enter** to confirm the action or **n** to cancel.

Examples

The following example shows a CE session being opened for a CE network module in slot 2:

```
Router# service-module content-engine 2/0 session
Trying 10.10.10.1, 2129 ... Open
CE-netmodule con now available
Press RETURN to get started!
CE-netmodule> enable
CE-netmodule#
```

The following example clears the session that had been used to configure the CE in the network module in slot 1:

```
Router# service-module content-engine 1/0 session clear
[confirm]
 [OK]
```

Related Commands

Command	Description
interface content-engine	Configures an interface for a CE network module and enters interface configuration mode.
show controllers content-engine	Displays controller information for CE network modules.
show interfaces content-engine	Displays basic interface configuration information for a CE network module.

service-module content-engine shutdown

To gracefully halt a content engine (CE) network module, use the **service-modulecontent-engineshutdown** command in privileged EXEC mode.

service-module content-engine *slot/unit* **shutdown**

Syntax Description

slot	Number of the router chassis slot for the network module.
/ *unit*	Number of the daughter card on the network module. For CE network modules, always use 0. The slash mark is required between the *slot* argument and the *unit*argument.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)YT	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

At the confirmation prompt, press **Enter** to confirm the action or **n** to cancel.

The **service-modulecontent-engineshutdown** command brings down the operating system of the specified content engine network module in an orderly fashion to protect the network module's hard drive. When the system has been shut down, the network module can be removed from the router.

Examples

The following example gracefully halts the CE network module in slot 1:

```
Router# service-module content-engine 1/0 shutdown
Shutdown is used for Online removal of Service Module.
Do you want to proceed with shutdown?[confirm]
Use service module reset command to recover from shutdown.
```

Related Commands

Command	Description
interface content-engine	Configures an interface for a CE network module and enters interface configuration mode.
service-module content-engine reload	Performs a graceful halt and reboot of a CE network module operating system.
service-module content-engine reset	Resets the hardware on a CE network module.
show controllers content-engine	Displays controller information for CE network modules.
show interfaces content-engine	Displays basic interface configuration information for a CE network module.

service-module content-engine status

To display configuration information related to the hardware and software on the content engine (CE) side of a CE network module, use the **service-modulecontent-enginestatus**command in privileged EXEC mode.

service-module content-engine *slot* / *unit* **status**

Syntax Description

slot	Number of the router chassis slot for the network module.
/ *unit*	Number of the daughter card on the network module. For CE network modules, always use 0. The slash mark is required between the *slot* argument and the *unit*argument.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)YT	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

Use the **service-modulecontent-enginestatus** command to:

- Display the CE network module software release version.
- Check the CE network module status (steady or down).
- Display hardware information for the CE network module including CPU, memory, interface, and disk drive information.

Examples

The following example displays information for a CE network module in router slot 1:

```
Router# service-module content-engine 1/0 status
Service Module is Cisco Content-Engine1/0
Service Module supports session via TTY line 33
Service Module is in Steady state
Getting status from the Service Module, please wait..
Application and Content Networking Software (ACNS)
Copyright (c) 1999-2002 by Cisco Systems, Inc.
Application and Content Networking Software Release 4.2.2 (build b3 May  6 2002)
Version: ce2636-sw-<unknown-version>
Compiled 18:03:40 May  6 2002 by engineer
Compile Time Options: PP
System was restarted on Mon Jan  7 20:30:37 1980.
The system has been up for 8 minutes, 30 seconds.
Core CPU is GenuineIntel Pentium III (Coppermine) (rev 8) running at 498MHz.
246 Mbytes of Physical memory.
2 FastEthernet interfaces
1 Console interface
List of disk drives:
disk00: Normal          (h00 c00 i00 l00)    19075MB( 18.6GB)
```

Related Commands

Command	Description
interface content-engine	Configures an interface for a CE network module and enters interface configuration mode.
show controllers content-engine	Displays controller information for CE network modules.
show interfaces content-engine	Displays basic interface configuration information for a CE network module.

service-module external ip address

To define the IP address for the external LAN interface on a content engine (CE) network module, use the **service-moduleexternalipaddress**command in content-engine interface configuration mode. To delete the IP address associated with this interface, use the **no** form of this command.

service-module external ip address *external-ip-addr subnet-mask*
no service-module external ip address

Syntax Description

external-ip-addr	IP address of the external LAN interface on a CE network module.
subnet-mask	Subnet mask to append to the IP address.

Command Default

No default behavior or values

Command Modes

Content-engine interface configuration

Command History

Release	Modification
12.2(11)YT	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Examples

The following example defines an IP address for the external LAN interface on the CE network module in slot 1:

```
Router(config)# interface content-engine 1/0
Router(config-if)# service-module external ip address
 172.18.12.28 255.255.255.0
Router(config-if)# exit
```

Related Commands

Command	Description
interface content-engine	Configures an interface for a CE network module and enters interface configuration mode.
show controllers content-engine	Displays controller information for CE network modules.
show interfaces content-engine	Displays basic interface configuration information for a CE network module.

service-module heartbeat-reset disable

To disable the service module from being reset when the heartbeat is lost, use the service-module heartbeat-reset disable command in configuration interface mode. To allow a reset of the service module when no heartbeat is received, use the **no** form of this command.

service-module heartbeat-reset disable
no service-module heartbeat-reset disable

Syntax Description

This command has no arguments or keywords.

Command Default

Heartbeat reset is enabled.

Command Modes

Configuration interface (config-if)

Command History

Release	Modification
15.1(4)M	This command was introduced.

Usage Guidelines

With the existing IOS code, if no heartbeat is received from a service module after a period of time, the IOS resets the service module. For some applications, this reset function should be disabled because it blocks normal operations.

This command, being a configuration mode command, persists through router reloads.

Alternatively, the service-module ism heartbeat-reset disable command and the service-module sm heartbeat-reset disable command can prevent Cisco IOS software from rebooting the internal service module (ISM) and the SM-SRE service module, respectively, when the heartbeat is lost. However, both these commands are EXEC mode commands and they are lost when the router reboots.

Examples

The following example shows how to disable the heartbeat reset:

```
Router(config)# interface sm 1/0
Router(config-if)# service-module heartbeat-reset disable
```

Related Commands

Command	Description
service-module	Sets service module parameters.
service-module ism heartbeat-reset	Prevents Cisco IOS software from rebooting the ISM when the heartbeat is lost.
service-module sm heartbeat-reset	Prevents Cisco IOS software from rebooting the SM-SRE service module when the heartbeat is lost.

service-module ids-sensor

To reboot, reset, enable console access to, shutdown, and monitor the status of the Cisco Intrusion Detection System (IDS) network module, use the **service-moduleids-sensor** command in privileged EXEC mode.

service-module ids-sensor *slot/port* {**reload** | **reset** | **session** | **shutdown** | **status**}

Syntax Description

slot	Number of the router chassis slot for the network module.
/ *port*	Port number of the network module. For Cisco IDS network modules, always use 0. The slash mark is required between the *slot* argument and the *unit*argument.
reload	Performs a graceful halt and reboot of the operating system on a Cisco IDS network module.
reset	Resets the hardware on the Cisco IDS network module. This command is usually used to recover from a shutdown.
session	Enables console access to the Cisco IDS network module from the router.
shutdown	Shuts down the IDS applications that are running on a Cisco IDS network module.
status	Provides information on the status of the Cisco IDS software.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

If a confirmation prompt is displayed, press **Enter** to confirm the action or **n** to cancel.

The Cisco IDS network module is also referred to as the NM-CIDS.

Examples

The following example gracefully halts and reboots the operating system on the Cisco IDS network module in slot 1:

```
Router# service-module ids-sensor 1/0 reload
Do you want to proceed with reload?[confirm]
```

The following example resets the hardware on the Cisco IDS network module in slot 1. A warning is displayed.

```
Router# service-module ids-sensor 1/0 reset
Use reset only to recover from shutdown or failed state
Warning: May lose data on the hard disk!
Do you want to reset?[confirm]
```

Caution Hard-disk drive data loss occurs only if you issue the reset command without first shutting down the Cisco IDS network module. You can use the reset command safely in other situations.

The following example enables console access to the Cisco IDS network module operating system in slot 1:

```
Router# service-module ids-sensor 1/0 session
```

The following example shuts down IDS applications that are running on the Cisco IDS network module in slot 1:

```
Router# service-module ids-sensor 1/0 shutdown
Trying 10.10.10.1, 2129 ... Open
%SERVICEMODULE-5-SHUTDOWN2:Service module IDS-Sensor1/0 shutdown complete
```

The following example shows the status of the Cisco IDS software:

```
Router# service-module ids-sensor 1/0 status
Service Module is Cisco IDS-Sensor1/0
Service Module supports session via TTY line 33
Service Module is in Steady state
Getting status from the Service Module, please wait...
Service Module Version information received, Major ver = 1, Minor ver= 1
Cisco Systems Intrusion Detection System Network Module
Software version: 4.1(1)S42(0.3)
Model: NM-CIDS
Memory: 254676 KB
```

Related Commands

Command	Description
ids-service-module monitoring	Enables IDS monitoring on a specified interface.

service-module integrated-service-engine default-boot

To configure the integrated-service-engine (ISE) network module to use the default BIOS and bootloader, use the service-module integrated-service-engine **default-boot** command in privileged EXEC mode.

service-module integrated-service-engine slot/unit default-boot

Syntax Description

slot	Number of the router chassis slot for the network module.
unit	Number of daughter cards on the network module, if included. For ISE network modules, always use 0.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(9)T	This command was introduced for the ISE network module.

Examples

After a downtime event or failed upgrade, use the service-module integrated**-service-engineslot/unitdefault-boot** command to configure the network module to use the primary BIOS and primary bootloader to perform startup routines.

The following is sample output from the **integrated-service-engineslot/unitdefault-boot** command for a port adapter in chassis slot 2 on a Cisco router:

```
Router# service-module integrated-service-engine 2/0 default-boot
clear  Clear Default Boot
set    Set Default Boot

Router# service-module integrated-service-engine 2/0 default-boot clear
Router# service-module integrated-service-engine 2/0 default-boot set
```

service-module integrated-service-engine reload

To perform a graceful shutdown and reboot of the integrated-service-engine (ISE) network module operating system, use the **service-moduleintegrated-service-enginereload** command in privileged EXEC mode.

service-module integrated-service-engine *slot/unit* **reload**

Syntax Description

slot	Number of the router chassis slot for the network module.
/ *unit*	Number of the daughter card on the network module. For ISE network modules, always use 0. The slash mark (/) is required between the *slot* argument and the *unit*argument.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(9)T	This command was introduced for ISE network modules.

Usage Guidelines

At the confirmation prompt, press **Enter** to confirm the action or **n** to cancel.

Examples

The following example gracefully shuts down and reboots the ISE network module's operating system in slot 1:

```
Router# service-module integrated-service-engine 1/0 reload
Do you want to proceed with reload?[confirm]
```

Related Commands

Command	Description
interface integrated-service-engine	Configures an interface for ISE network modules and enters interface configuration mode.
service-module integrated-service-engine reset	Resets the hardware on ISE network modules.
service-module integrated-service-engine shutdown	Gracefully shuts down ISE network modules.
show diag	Displays controller information for ISE network modules.
show interfaces integrated-service-engine	Displays basic interface configuration information for ISE network modules.

service-module integrated-service-engine reset

To reset the integrated-service-engine (ISE) network module hardware, use the **service-moduleintegrated-service-enginereset** command in privileged EXEC mode.

service-module integrated-service-engine *slot/unit* **reset**

Syntax Description

slot	Number of the router chassis slot for the network module.
/ *unit*	Number of the daughter card on the network module. For ISE network modules, always use 0. The slash mark (/) is required between the *slot* argument and the *unit*argument.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(9)T	This command was introduced for ISE network modules.

Usage Guidelines

At the confirmation prompt, press **Enter** to confirm the action or **n** to cancel.

Caution Because you may lose data, use the **service-moduleintegrated-service-enginereset** command only to recover from a shutdown or failed state.

Examples

The following example resets the hardware on the ISE network module in slot 1:

```
Router# service-module integrated-service-engine 1/0 reset
Use reset only to recover from shutdown or failed state
Warning: May lose data on the hard disk!
Do you want to reset?[confirm]
```

Related Commands

Command	Description
interface integrated-service-engine	Configures an interface for ISE network modules and enters interface configuration mode.
service-module integrated-service-engine reload	Performs a graceful shutdown and reboot on the ISE network module operating system.
service-module integrated-service-engine shutdown	Gracefully shuts down ISE network modules.
show diag	Displays controller information for ISE network modules.

Command	Description
show interfaces integrated-service-engine	Displays basic interface configuration information for ISE network modules.

service-module integrated-service-engine session

To begin a configuration session with an integrated-service-engine (ISE) network module through a console connection, use the **service-moduleintegrated-service-enginesession** command in privileged EXEC mode.

service-module integrated-service-engine *slot/unit* **session** [**clear**]

Syntax Description

slot	Number of the router chassis slot for the network module.
/ *unit*	Number of the daughter card on the network module. For ISE network modules, always use 0. The slash mark (/) is required between the *slot* argument and the *unit*argument.
clear	(Optional) Clears the ISE configuration session.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(9)T	This command was introduced for ISE network modules.

Usage Guidelines

Only one session at a time is allowed into the network module from the internal ISE network-module-side interface.

After starting a session, you can perform any ISE configuration task. You first access the ISE console in a user-level shell. To access the privileged EXEC command shell, where most commands are available, use the **enable** command.

After you finish ISE configuration and exit the ISE console session, use this command with the **clear** keyword to clear the session. At the confirmation prompt, press **Enter** to confirm the action or **n** to cancel.

Examples

The following example shows an ISE session being opened for an ISE network module in slot 2:

```
Router# service-module integrated-service-engine 2/0 session
Trying 10.10.10.1, 2129 ... Open
ISE-netmodule con now available
Press RETURN to get started!
ISE-netmodule> enable
ISE-netmodule#
```

The following example clears the session that had been used to configure the ISE in the network module in slot 2:

```
Router# service-module integrated-service-engine 1/0 session clear
[confirm]
 [OK]
```

Related Commands

Command	Description
enable	Enters prviledged EXEC mode.
interface	Configures an interface and enters interface configuration mode.
show diag	Displays controller information for a network module.
show interface integrated-service engine	Displays basic interface configuration information for network modules.

service-module integrated-service-engine shutdown

To gracefully shut down an integrated-service-engine (ISE) network module, use the **service-moduleintegrated-service-engineshutdown** command in privileged EXEC mode.

service-module integrated-service-engine *slot/unit* **shutdown**

Syntax Description

slot	Number of the router chassis slot for the network module.
/ *unit*	Number of the daughter card on the network module. For ISE network modules, always use 0. The slash mark (/) is required between the *slot* argument and the *unit*argument.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(9)T	This command was introduced for ISE network modules.

Usage Guidelines

At the confirmation prompt, press **Enter** to confirm the action or **n** to cancel.

The **service-moduleintegrated-service-engineshutdown** command brings down the operating system of the specified integrated-service-engine network module in an orderly fashion to protect the hard drive. When the system has been shut down, the module can be removed from the router.

Examples

The following example gracefully shuts down the ISE network module in slot 1:

```
Router# service-module integrated-service-engine 1/0 shutdown
Shutdown is used for Online removal of Service Module.
Do you want to proceed with shutdown?[confirm]
Use service module reset command to recover from shutdown.
```

Related Commands

Command	Description
interface integrated-service-engine	Configures an interface for ISE network modules and enters interface configuration mode.
service-module integrated-service-engine reload	Performs a graceful shut down and reboot of an ISE network module operating system.
service-module integrated-service-engine reset	Resets the hardware on ISE network modules.
show diag	Displays controller information for ISE network modules.
show interfaces integrated-service-engine	Displays basic interface configuration information for ISE network modules.

service-module integrated-service-engine status

To display configuration information related to the hardware and software on the integrated-service-engine (ISE) side of a network module, use the **service-moduleintegrated-service-enginestatus**command in privileged EXEC mode.

service-module integrated-service-engine *slot*/*unit* **status**

Syntax Description

slot	Number of the router chassis slot for the network module.
/ *unit*	Number of the daughter card on the network module. For ISE network modules, always use 0. The slash mark (/) is required between the *slot* argument and the *unit*argument.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(9)T	This command was introduced for ISE network modules.

Usage Guidelines

Use the **service-moduleintegrated-service-enginestatus** command to

- Display the ISE network module's software release version
- Check the ISE network module status (steady or down)
- Display hardware information for the ISE network module, including CPU, memory, interface, and disk drive information

Examples

The following example displays information for an ISE network module in router slot 1:

```
Router# service-module integrated-service-engine 1/0 status
Service Module is Cisco integrated-service-engine1/0
Service Module supports session via TTY line 33
Service Module is in Steady state
Getting status from the Service Module, please wait..
Application and Content Networking Software (ACNS)
Copyright (c) 1999-2002 by Cisco Systems, Inc.
Application and Content Networking Software Release 4.2.2 (build b3 May  6 2002)
Version: ce2636-sw-<unknown-version>
Compiled 18:03:40 May  6 2002 by engineer
Compile Time Options: PP
System was restarted on Mon Jan  7 20:30:37 1980.
The system has been up for 8 minutes, 30 seconds.
Core CPU is GenuineIntel Pentium III (Coppermine) (rev 8) running at 498MHz.
246 Mbytes of Physical memory.
2 FastEthernet interfaces
1 Console interface
List of disk drives:
disk00: Normal          (h00 c00 i00 l00)    19075MB( 18.6GB)
```

Related Commands

Command	Description
interface integrated-service-engine	Configures an interface for ISE network modules and enters interface configuration mode.
show diag	Displays controller information for ISE network modules.
show interfaces integrated-service-engine	Displays basic interface configuration information for ISE network modules.

service-module integrated-service-engine statistics

To display reset and reload information for an integrated-service-engine (ISE) network module and its Cisco IOS software, use the **service-moduleintegrated-service-enginestatistics**command in EXEC mode.

service-module integrated-service-engine *slot/port* **statistics**

Syntax Description

module	Designates a specific ISE network module installed in the router.
slot	Designates the slot where the selected ISE network module is installed in the router.

Command Default

none

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
12.4(9)T	This command was introduced for ISE network modules.

Examples

The following example displays information for an ISE network module in an access router for slot 2:

```
Router# service-module integrated-service-engine 2/0 statistics
Module Reset Statistics:
  CLI reset count = 1
  CLI reload count = 0
  Registration request timeout reset count = 0
  Error recovery timeout reset count = 0
  Module registration count = 2
The last IOS initiated event was a cli reset at *13:34:33.847 UTC Sun Dec 18 2005
```

service-module ip address

To define the IP address for the internal network-module-side interface on a content engine network module (NM-CE-BP), Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT), Cisco cable modem high-speed WAN interface card (HWIC-CABLE-D-2, HWIC-CABLE-E/J-2), or the Cisco Services Ready Engine (Cisco SRE) modules (SM-SRE-XXX-K9, ISM-SRE-XXX-K9) use the **service-moduleipaddress** command in content-engine interface configuration mode, satellite interface configuration mode, content-engine configuration mode, or service-module interface configuration mode. To delete the IP address associated with this interface, use the **no** form of this command.

service-module ip address *nm-side-ip-addr subnet-mask* [*"string"*]
no service-module ip address [*"string"*]

Syntax Description

nm-side-ip-addr	IP address of the internal network-module-side interface on a CE network module (NM-CE-BP), Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT), or Cisco cable modem high-speed WAN interface card (HWIC-CABLE-D-2, HWIC-CABLE-E/J-2).
subnet-mask	Subnet mask to append to the IP address.
string	(Optional) Name of the virtual interface on the module side that will be assigned the IP address. The string must be in quotes. This argument is available on Cisco SRE modules only.

Command Default

The well-known diagnostic IP address of 192.168.100.1, is supported on all physical interfaces associated with the cable modem to CPE interface (CMCI).

Command Modes

Content-engine interface configuration Satellite interface configuration Cable-modem interface configuration Service-module interface configuration

Command History

Release	Modification
12.2(11)YT	This command was introduced for the CE network module.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3(14)T	This command was implemented for the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT).
12.4(6)XE	This command was implemented for the Cisco cable modem high-speed WAN interface card (HWIC-CABLE-D-2, HWIC-CABLE-E/J-2).
15.1(4)M	The optional *string* argument was added on Cisco SRE modules only.

Usage Guidelines

Content Engine Network Module (NM-CE-BP)

There are no usage guidelines for this command.

Cisco IP VSAT Satellite WAN Network Module (NM-1VSAT-GILAT)

For the NM-1VSAT-GILAT network module, the **service-moduleipaddress** command is typically not used. The NM-1VSAT-GILAT network module IP address is automatically configured when you enter the **ipaddress** command in satellite interface configuration mode to configure the IP address and subnet mask of the router satellite interface with these conditions:

- The IP address leaves a remainder of 2 when the last octet is divided by 4.
- The subnet mask has /30 or fewer masking bits.

If you use this method to configure the IP address for the router satellite interface, the system automatically configures the IP address and subnet mask on the NM-1VSAT-GILAT network module with these results:

- The IP address is 1 less than the IP address you configured for the router satellite interface.
- The subnet mask is /30.

You can override the automatically configured IP address and mask by manually entering the **service-moduleipaddress** command.

Note The automatically configured IP address does not appear in the router configuration, because the **service-moduleipaddress** command is considered to be set to its default value. Similarly, if you manually configure an IP address and subnet mask that are identical to the automatically configured IP address and subnet mask, the **service-moduleipaddress** command does *not* appear in the router configuration.

Cisco Cable Modem High-Speed WAN Interface Card (HWIC-CABLE-D-2, HWIC-CABLE-E/J-2)

There are no usage guidelines for this command.

Cisco SRE Modules (SM-SRE-XXX-K9, ISM-SRE-XXX-K9)

In Cisco IOS Release 15.1(4)M and later releases, the Cisco SRE modules support an optional "*string*" argument to this command to allow for multiple IP addresses to be configured on the module side. The application running on the SRE module can accept or reject the applied configuration.

Examples

This section provides the following examples:

Content Engine Network Module (NM-CE-BP) Example

The following example shows how to define an IP address for the internal network-module-side interface on the CE network module in slot 1:

```
Router(config)# interface content-engine 1/0
Router(config-if)# service-module ip address 172.18.12.26 255.255.255.0
Router(config-if)# exit
```

Cisco IP VSAT Satellite WAN Network Module (NM-1VSAT-GILAT) Example--Manually Configuring the IP Address

In the following example, the router satellite interface is assigned an IP address (10.0.0.7), the last octet of which does *not* leave a remainder of 2 when divided by 4. The system displays a message to manually configure the IP address for the NM-1VSAT-GILAT network module. Notice that the IP addresses for both the router satellite interface and the NM-1VSAT-GILAT network module appear in the running configuration.

```
Router(config)# interface satellite 1/0

Router(config-if)# ip address 10.0.0.7 255.255.255.0

%VSAT-6-PIMINCOMPADDR:The IP address configured on Satellite1/0
      requires a manually configured IP address for the satellite module
Router(config-if)# service-module ip address 10.0.0.6 255.255.255.0
Router(config-if)# end

Router# show running-config | begin Satellite

interface Satellite 1/0
   ip address 10.0.0.7 255.255.255.0
   service-module ip address 10.0.0.6 255.255.255.0
```

Cisco IP VSAT Satellite WAN Network Module (NM-1VSAT-GILAT) Example--Using the Automatically Configured IP Address

In the following example, the router satellite interface IP address is configured as 10.0.0.6. Because the last octet of the IP address leaves a remainder of 2 when divided by 4, the system automatically configures the IP address for the NM-1VSAT-GILAT network module.

Although the NM-1VSAT-GILAT network module IP address and mask do not appear in the router configuration, you know that the IP address is 1 less than the IP address of the router satellite interface and has a subnet mask of /30. In this case, the NM-1VSAT-GILAT network module is automatically configured with the following IP address and mask: 10.0.0.5 255.255.255.252.

```
!
interface Satellite 1/0
 ip address 10.0.0.6 255.255.255.0
!
```

Cisco IP VSAT Satellite WAN Network Module (NM-1VSAT-GILAT) Example--Overriding the Automatically Configured IP Address

In the following example, the router satellite interface IP address is configured as 10.0.0.6. Because the last octet of the IP address leaves a remainder of 2 when divided by 4, the system automatically configures the IP address and mask for the NM-1VSAT-GILAT network module as 10.0.0.5 255.255.255.252.

Nevertheless, the NM-1VSAT-GILAT network module IP address and mask are manually configured as 10.0.0.1 255.255.255.0 to override the automatically derived IP address and mask. Notice that the IP addresses for both the router satellite interface and the NM-1VSAT-GILAT network module appear in the running configuration.

```
!
interface Satellite 1/0
 ip address 10.0.0.6 255.255.255.0
 service-module ip address 10.0.0.1 255.255.255.0
!
```

Cisco Cable Modem High-Speed WAN Interface Cards (HWIC-CABLE-D-2, HWIC-CABLE-E/J-2) Example

The following example shows how to define an IP address for the cable modem interface in slot 0:

```
Router(config)# interface cable-modem 0

Router(config-if)# service-module ip address 172.18.12.26 255.255.255.0

Router(config-if)# exit
```

Cisco SRE Module (ISM-SRE-XXX-K9, SM-SRE-XXX-K9) Example

The following example shows how to define an IP address for the service module interface in slot 3:

```
Router(config)# interface SM 3/0

Router(config-if)# service-module ip address 172.18.12.26 255.255.255.0

Router (config-if)# service-module ip address 172.18.12.27 255.255.255.0 “VirtualMachine1”
Router (config-if)# service-module ip address 172.18.12.28 255.255.255.0 “VirtualMachine2”
Router(config-if)# exit
```

Related Commands

Command	Description
show controllers content-engine	Displays controller information for CE network modules.
show controllers satellite	Displays controller information about the internal router interface that connects to an installed Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT).
show interfaces satellite	Displays general interface settings and traffic rates for the internal router interface that connects to an installed Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT).
show interfaces content-engine	Displays basic interface configuration information for a CE network module.

service-module ip default-gateway

To define a default gateway (router) for a content engine (CE) network module, use the **service-moduleipdefault-gateway**command in content-engine interface configuration mode. To remove the default gateway from the CE configuration, use the **no** form of this command.

service-module ip default-gateway *gw-ip-addr*
no service-module ip default-gateway

Syntax Description

gw-ip-addr	IP address of the default gateway.

Command Default

No default behavior or values

Command Modes

Content-engine interface configuration

Command History

Release	Modification
12.2(11)YT	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Examples

The following example configures a default gateway for the CE network module in slot 1:

```
Router(config)# interface content-engine
 1/0
Router(config-if)# service-module ip default-gateway
 172.18.12.1
Router(config-if)# exit
```

Related Commands

Command	Description
interface content-engine	Configures an interface for a CE network module and enters interface configuration mode.
show controllers content-engine	Displays controller information for CE network modules.
show interfaces content-engine	Displays basic interface configuration information for a CE network module.

service-module ip redundancy

To link the primary HSRP interface status to that of the satellite interface, use the **service-module ip redundancy** command in satellite interface configuration mode. To remove the link between the primary HSRP interface status and the satellite interface status, use the **no** form of this command.

service-module ip redundancy *group-name*
no service-module ip redundancy *group-name*

Syntax Description

group-name	Name of the hot standby group. This name must match the hot standby group name configured for the primary HSRP interface, which is typically an Ethernet interface.

Command Default

HSRP is disabled.

Command Modes

Satellite interface configuration (config-if)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **service-module ip redundancy** command only when you have two Cisco IP VSAT satellite WAN network modules (NM-1VSAT-GILAT) on separate HSRP-redundant routers that connect to the same outdoor unit (ODU).

This command enables the satellite interface to spoof the line protocol UP state.

Examples

The following example shows how to link the primary HSRP interface status to that of the satellite interface:

```
Router (config-if)# service-module ip redundancy grp-hsrp
```

Related Commands

Command	Description
standby ip	Activates HSRP.
standby name	Configures the name of the hot standby group.
standby preempt	Enables preemption on the router and optionally configures a preemption delay.
standby track	Configures an interface so that the hot standby priority changes based on the availability of other interfaces.

service-module ism default-boot

To configure the internal service module (ISM) to use the default BIOS and bootloader, use the **service-moduleismdefault-boot** command in privileged EXEC mode.

service-module ism *slot/port* **default-boot**

Syntax Description

slot	Router slot in which the service module is installed. For internal service modules, always use 0.
/ *port*	Port number of the module interface. Always use 0. The slash mark (/) is required.

Command Default

The default BIOS and bootloader are not used by the ISM.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

After a downtime event or failed upgrade, use this command to configure the service module to use the primary BIOS and primary bootloader to perform startup routines.

Examples

The following is sample output for an ISM:

```
Router# service-module ism 0/0 default-boot
clear  Clear Default Boot
set    Set Default Boot

Router# service-module ism 0/0 default-boot clear
Router# service-module ism 0/0 default-boot set
```

service-module ism heartbeat-reset

To prevent Cisco IOS software from rebooting the internal service module (ISM) when the heartbeat is lost, use the **service-moduleismheartbeat-reset** command in privileged EXEC mode.

service-module ism *slot/port* **heartbeat-reset** {**disable** | **enable**}

Syntax Description

slot	Number of the router slot in which the service module is installed. For internal service modules, always use 0.
/ *port*	Port number of the module interface. Always use 0. The slash mark (/) is required.
disable	Disables reset of the ISM if the heartbeat is lost.
enable	Enables reset of the ISM if the heartbeat is lost.

Command Default

ISM is reset when heartbeat is lost.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

When the ISM is booted in fail-safe mode or is undergoing an upgrade, this command prevents a reboot during the process.

When the ISM heartbeat is lost, the router applies a fail-open or fail-close configuration option to the module, stops sending traffic to the module, and sets the module to error state. The router performs a hardware reset on the ISM and monitors it until the heartbeat is reestablished.

Examples

The following example shows how to disable the ISM from being reset if the heartbeat is lost:

```
Router# service-module ism 0/0 heartbeat-reset disable
```

You can display the status of the heartbeat reset feature with the **service-moduleismstatus**command:

```
Router# service-module ism 0/0 status

Service Module is Cisco IDS-Sensor 0/0
Service Module supports session via TTY line 194
Service Module heartbeat-reset is enabled <=====
```

Related Commands

Command	Description
interface ism	Configures an interface for an ISM and enters interface configuration mode.
service-module ism reload	Performs a graceful shutdown and reboot of the ISM.

Command	Description
service-module ism reset	Resets the ISM hardware.
service-module ism shutdown	Performs a graceful shutdown of the ISM.
service-module ism status	Displays configuration information related to the hardware and software on an ISM.

service-module ism install

To use Cisco SRE to install an application on a internal service module (Cisco ISM-SRE), use the **service-moduleisminstall**command in privileged EXEC configuration mode.

service-module ism *slot/port* **install url** *url* [**script** *filename*] [**argument** *"string"*] [**force**]

Syntax Description

slot/port	Location of the services engine module in the router. For internal service modules, the slot and port number must be 0.
url *url*	Address of FTP or HTTP server, as defined in RFC 2396, on which application packages and Tcl scripts are located.
script	(Optional) Changes name of Tcl script to be run from default value to script specified by *filename* argument.
filename	Name of Tcl script.
argument	(Optional) Installer will not present options for the variable specified in the *string* argument.
“ *string* **”**	Alphanumeric characters of variable to be passed directly to the Tcl script via the command line. Variable must be enclosed in quotation marks (“ ”)
force	(Optional) Tcl script automatically proceeds with install without prompting for user input.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

This command uses a common module-dependent bootloader to install a Linux-based application, such as Cisco Unity Express or Cisco AXP, on an internal service module (Cisco ISM-SRE).

The slash mark (/) is required between the *slot* argument and the *port* argument.

You can only issue one instance of this command at a time on a router. You cannot use this command to install an application on two or more services engine modules in the same router at a time.

The Tcl script to be run must reside in the same FTP or HTTP server and directory as the application packages to be installed. If a credential is required, the user name and password must be imbedded in the url as shown in the following example:

```
Router# service-module ism 0/0 install url ftp://username:passwd@server.com/axp
```

If two or more of the optional keyword/argument combinations are used with this command, they must be issued in the order presented in the command syntax. For example, you cannot use the **force** keyword before the **script** or**argument** keywords, nor the **argument** keyword before the **script** keyword, when you issue this command.

Use the **script***filename* keyword/argument combination with this command to specify that the Cisco IOS software use some Tcl script other than the default installer during the installation.

Use the **argument“***string***”** keyword/argument combination with this command to manually provide variables during installation process and bypass the user interaction feature of the installer. The variable must include the left and right quotation marks (“ ”).

Use the **force** keyword with this command to install an application without prompting for user input. If you use this keyword and if the application requires you to provide certain variables during the installation, you should also use the **argument“***string***”** keyword/argument combination to manually provide the required variables because the **force** keyword will direct the installer to bypass all user interaction during the installation.

To stop the install while the Tcl script is being downloaded, use the **service-moduleisminstallabort**command. This command cannot be used once the actual installation begins.

Examples

The following example shows how to use this command to run the “help.sre” Tcl script rather than the default installation Tcl script:

```
Router# service-module ism 0/0 install url ftp://server.com/cue script help.sre
Router#
```

The following example shows how to direct the installer to use the specified language variable for US English instead of prompting you with language options for Cisco Unity Express:

```
Router# service-module ism 0/0 install url ftp://server.com/cue argument “lang=en_us”
Router#
```

The following example shows the messages displayed on the module console during a successful installation using Cisco SRE:

```
Feb  6 19:09:22.526 EDT: %SM_INSTALL-6-INST_PROG: Service-Module-ISM 0/0 PROGRESSING:
Validating package signature ...1 .
Feb  6 19:09:23.058 EDT: %SM_INSTALL-6-INST_PROG: Service-Module-ISM 0/0 PROGRESSING: Parsing
 package manifest files ...1 .
Feb  6 19:09:44.742 EDT: %SM_INSTALL-6-INST_PROG: Service-Module-ISM 0/0 PROGRESSING:
Starting payload download1 .
Feb  6 19:09:52.022 EDT: %SM_INSTALL-6-INST_PROG: Service-Module-ISM 0/0 PROGRESSING:
Performing Hot install ...1 .
Install successful on Service-Module-ISM 0/0 Feb  6 19:10:28.826 EDT: %SM_INSTALL-6-INST_SUCC:
 Service-Module-ISM 0/0 SUCCESS: install-completed .
```

Related Commands

Command	Description
service-module ism install abort	Stops the install process and returns to the boot-loader prompt.
service-module ism uninstall	Uses Cisco SRE to uninstall an SRE-supported application on an SRE-enabled services engine module.

service-module ism install abort

To abort the Cisco SRE install process on a Cisco ISM-SRE, use the **service-moduleisminstallabort**command in privileged EXEC configuration mode.

service-module ism *slot/port* **install abort** [**force**]

Syntax Description

slot/port	Location of the services engine module in the router. For internal service modules, the slot and port number must be 0.
force	(Optional) Tcl script automatically stops the installation without prompting for confirmation.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

This command stops the installation during the downloading portion of the process only. You cannot use this command to stop the process once the actual installation has begun.

Use the **force** keyword with this command to stop the process without first prompting for confirmation.

Examples

The following example shows how to use this command to stop an application installation without first prompting for confirmation:

```
Router# service-module ism 0/0 install abort force
.
.
.
boot-loader>
```

Related Commands

Command	Description
service-module ism install	Uses Cisco SRE to install an SRE-supported application on an SRE-enabled services engine module.

service-module ism reload

To perform a graceful shutdown and reboot of the internal service module (ISM) operating system, use the **service-moduleismreload** command in privileged EXEC mode.

service-module ism *slot*/*port* **reload**

Syntax Description

slot	Router slot in which the service module is installed. For internal service modules, always use 0.
/ *port*	Port number of the module interface. Always use 0. The slash mark (/) is required.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced for ISMs.

Usage Guidelines

At the confirmation prompt, press **Enter** to confirm the action or **n** to cancel.

Examples

The following example shows how to gracefully shut down and reboot the ISM operating system:

```
Router# service-module ism 0/0 reload

Do you want to proceed with reload?[confirm]
```

Related Commands

Command	Description
interface ism	Configures an interface for an ISM and enters interface configuration mode.
service-module ism reset	Resets the ISM hardware.
service-module ism shutdown	Gracefully shuts down the ISM.
show diag	Displays controller information for ISMs.
show interfaces ism	Displays basic interface configuration information for ISMs.

service-module ism reset

To reset the internal service module (ISM) hardware, use the **service-moduleismreset** command in privileged EXEC mode.

service-module **ism** *slot*/*port* **reset**

Syntax Description

slot	Router slot in which the service module is installed. For internal service modules, always use 0.
/ *port*	Port number of the module interface. Always use 0. The slash mark (/) is required.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced for ISMs.

Usage Guidelines

At the confirmation prompt, press **Enter** to confirm the action or **n** to cancel.

Caution Because you may lose data, use the **service-moduleismreset** command only to recover from a shutdown or failed state.

Examples

The following example shows how to reset the ISM hardware:

```
Router# service-module ism 0/0 reset

Use reset only to recover from shutdown or failed state
Warning: May lose data on the the NVRAM, nonvolatile file system or unsaved configuration!
Do you want to reset?[confirm]
```

Related Commands

Command	Description
interface ism	Configures an interface for an ISM and enters interface configuration mode.
service-module ism reload	Performs a graceful shutdown and reboot of the ISM operating system.
service-module ism shutdown	Gracefully shuts down the ISM.
show diag	Displays controller information for ISMs.
show interfaces ism	Displays basic interface configuration information for ISMs.

service-module ism session

To begin a configuration session for an internal service module (ISM) through a console connection, use the **service-moduleismsession** command in privileged EXEC mode.

service-module ism *slot/port* **session** [**clear**]

Syntax Description

slot	Router slot in which the service module is installed. For internal service modules, always use 0.
/ *port*	Port number of the module interface. Always use 0. The slash mark (/) is required.
clear	(Optional) Clears the ISM configuration session.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

Only one session at a time is allowed into the service module from the ISM interface.

After starting a session, you can perform any ISM configuration task. You first access the ISM console in a user-level shell. To access the privileged EXEC command shell, where most commands are available, use the **enable** command.

After you finish configuration tasks and exit the ISM console session, use this command with the **clear** keyword to clear the session. At the confirmation prompt, press **Enter** to confirm the action or **n** to cancel.

Examples

The following example shows a session being opened for an ISM:

```
Router# service-module ism 0/0 session

Trying 10.10.10.1, 2129 ... Open

ISE-netmodule con now available
Press RETURN to get started!

ISE-netmodule> enable
ISE-netmodule#
```

The following example clears the session that had been used to configure the ISM in slot 0:

```
Router# service-module ism 0/0 session clear
[confirm]
 [OK]
```

Related Commands

Command	Description
enable	Enters privileged EXEC mode.

Command	Description
interface	Configures an interface and enters interface configuration mode.
show diag	Displays controller information for a service module.
show interface ism	Displays basic interface configuration information for service modules.

service-module ism shutdown

To gracefully shut down an internal service module (ISM), use the **service-moduleismshutdown** command in privileged EXEC mode.

service-module ism *slot*/*port* **shutdown**

Syntax Description

slot	Router slot in which the service module is installed. For internal service modules, always use 0.
/ *port*	Port number of the module interface. Always use 0. The slash mark (/) is required.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

At the confirmation prompt, press **Enter** to confirm the action or **n** to cancel.

This command brings down the operating system of the specified ISM in an orderly fashion to protect the hard drive. When the system has been shut down, the module can be removed from the router.

Examples

The following example shows how to gracefully shut down the ISM:

```
Router# service-module ism 0/0 shutdown

Do you want to proceed with shutdown?[confirm]
Use service module reset command to recover from shutdown.

WARNING: Confirm that the service-module status shows 'is Shutdown' before removing the
module or powering off the system !
```

Related Commands

Command	Description
interface ism	Configures an interface for an ISM and enters interface configuration mode.
service-module ism reload	Performs a graceful shut down and reboot of the ISM operating system.
service-module ism reset	Resets the hardware on the ISM.
show diag	Displays controller information for ISMs.
show interfaces ism	Displays basic interface configuration information for ISMs.

service-module ism statistics

To display reset and reload information for an internal service module (ISM) and its Cisco IOS software, use the **service-moduleismstatistics**command in EXEC mode.

service-module ism *slot* / *port* **statistics**

Syntax Description

slot	Router slot in which the service module is installed. For internal service modules, always use 0.
/ *port*	Port number of the module interface. Always use 0. The slash mark (/) is required.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Examples

The following example displays information for an ISM:

```
Router# service-module ism 0/0 statistics

Module Reset Statistics:
 CLI reset count = 0
 CLI reload count = 0
 Registration request timeout reset count = 0
 Error recovery timeout reset count = 0
 Module registration count = 1
```

Related Commands

Command	Description
interface ism	Configures an interface for an ISM and enters interface configuration mode.
service-module ism reload	Performs a graceful shutdown and reboot of the ISM operating system.
service-module ism reset	Resets the ISM hardware.
service-module ism shutdown	Gracefully shuts down the ISM.
show interfaces ism	Displays basic interface configuration information for ISMs.

service-module ism status

To display configuration information related to the hardware and software on an internal service module (ISM), use the **service-moduleismstatus**command in privileged EXEC mode.

service-module ism *slot*/*port* **status**

Syntax Description

slot	Router slot in which the service module is installed. For internal service modules, always use 0.
/ *port*	Port number of the module interface. Always use 0. The slash mark (/) is required.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

Use this command to:

- Display the ISMs software release version
- Check the ISM status (steady or down)
- Display hardware information for the ISM, including CPU, memory, and interface information

Examples

The following example displays information for an ISM:

```
Router# service-module ism 0/0 status

Service Module is Cisco ISM0/0
Service Module supports session via TTY line 323
Service Module is in Steady state
Service Module heartbeat-reset is enabled
Getting status from the Service Module, please wait..
Cisco Foundation Software 1.0
FNDN Running on ISM
No install/uninstall in progress
```

Related Commands

Command	Description
interface ism	Configures an interface for an ISM and enters interface configuration mode.
show diag	Displays controller information for service modules.
show interfaces ism	Displays basic interface configuration information for ISMs.

service-module ism uninstall

To use Cisco SRE to uninstall an application on an internal service module (Cisco ISM-SRE), use the **service-moduleismuninstall**command in privileged EXEC configuration mode.

service-module ism *slot/port* **uninstall** [**force**]

Syntax Description

slot / *port*	Location of the services engine module in the router. For internal service modules, the slot and port number must be 0.
force	(Optional) Tcl script automatically proceeds with uninstall without prompting for confirmation.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

This command completely erases the disk or compact flash on the SRE-enabled services engine module and removes the application keys. It does not remove application licenses.

The slash mark (/) is required between the *slot* argument and the *port*argument.

You can only issue one instance of this command at a time on a router. You cannot use this command to uninstall an application on two or more services engine modules in the same router at a time.

Use the **force** keyword with this command to uninstall an application without first prompting for confirmation.

Examples

The following example shows how to use this command to uninstall an application without first prompting for confirmation:

```
Router# service-module ism 0/0 uninstall force
Router#
```

Related Commands

Command	Description
service-module ism install	Uses Cisco SRE to install an SRE-supported application on an SRE-enabled services engine module.

service-module mgf ip address

To place the service module (Cisco SM-SRE or Cisco ISM-SRE) on a subnet, use the **service-modulemgfipaddress**command in interface configuration mode.

service-module mgf ip address *ip-address subnet-mask* [**vlan** *vlan-id*]

Syntax Description

ip-address	IP address of the module's MGF interface.
subnet-mask	Subnet mask to append to the IP address.
vlan *vlan-id*	(Optional) Number of the VLAN to be assigned. The valid range is from 2 to 4094.

Command Default

Service module is not placed on a subnet.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

Use this command without the **vlan***vlan-id*argument to configure the IP address on the module side for the default VLAN (VLAN 1). Use this command with the **vlan***vlan-id*argument to configure the IP address on the module side for VLANs other than VLAN 1.

Examples

The following example assigns IP addresses to the default VLAN of the port and VLAN 20:

```
Router(config)# interface sm 1/0
Router(config-if)# service-module mgf ip address 192.0.2.0
Router(config-if)# service-module mgf ip address 192.0.2.1 vlan 20
```

service-module mgf ip default-gateway

To define a default gateway (router) for a service module (Cisco SRE SM or Cisco SRE ISM), use the **service-modulemgfipdefault-gateway**command in interface configuration mode.

service-module mgf ip default-gateway *gateway-ip-address* [**vlan** *vlan-id*]

Syntax Description

gateway-ip-address	IP address of the module's default gateway.
vlan *vlan-id*	(Optional) Number of the VLAN to be assigned. The valid range is from 2 to 4094.

Command Default

Default gateway is not defined for a service module.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

Use this command without the **vlan***vlan-id*argument to configure the default gateway on the module side for the default VLAN (VLAN 1). Use this command with the **vlan***vlan-id*argument to configure the default gateway on the module side for VLANs other than VLAN 1.

Examples

The following example assigns 192.0.2.0 as the default gateway for VLAN 1:

```
Router(config)# interface sm 2/0
Router(config-if)# service-module mgf ip default-gateway 192.0.2.0
```

service-module mgf ipv6 address

To place the service module (Cisco SM-SRE or Cisco ISM-SRE) on a subnet, use the **service-modulemgfipv6address**command in interface configuration mode.

service-module mgf ipv6 address *ipv6-address* [**vlan** *vlan-id*]

Syntax Description

ipv6-address	IPv6 address of the module's MGF interface.
vlan-id	(Optional) Number of the VLAN to be assigned. The valid range is from 2 to 4094.

Command Default

IPv6 address is not configured on the service module.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

Use this command without the **vlan***vlan-id*argument to configure the IPv6 address on the module side for the default VLAN (VLAN 1). Use this command with the **vlan***vlan-id*argument to configure the IPv6 address on the module side for VLANs other than VLAN 1.

Examples

The following example assigns IPv6 addresses to the default VLAN of the port and VLAN 20:

```
Router(config)# interface sm 2/0
Router(config-if)# service-module mgf ipv6 address 2001:0DB8::/48
Router(config-if)# service-module mgf ipv6 address 2001:0DB8::/48 vlan 20
```

service-module routing redistribute

To enable the router to send its routing database to the satellite network central hub, use the **service-moduleroutingredistribute** command in satellite interface configuration mode. To prevent the router from sending its routing database over the satellite network, use the **no** form of this command.

service-module routing redistribute
no service-module routing redistribute

Syntax Description

This command has no arguments or keywords.

Command Default

The router is enabled to send its routing database to the hub.

Command Modes

Satellite interface configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The **service-moduleroutingredistribute** command is used on a VSAT router, that is, an earthbound modular access router equipped with a Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT) that connects to a satellite network. When VSAT route updates are enabled, the NM-1VSAT-GILAT network module uses Router Blade Configuration Protocol (RBCP) messages to communicate VSAT routing table changes to the hub.

Entering the **noservice-moduleroutingredistribute** command is useful when you do not want the hub to be aware of all the routes known by the VSAT router, such as when Network Address Translation (NAT) is configured on the router.

The hub must learn the remote VSAT routing database for the satellite network to function properly. Therefore, if you enter the **noservice-moduleroutingredistribute** command, then one of the following actions is required:

- You use RIPv2 as the only routing protocol on your VSAT router. The hub can understand and track RIPv2 route updates.
- On the hub router, configure static routes to the VSAT router networks.

Examples

The following example shows how to prevent the VSAT router from sending its routing database to the satellite network central hub:

```
Router(config-if)# no service-module routing redistribute
```

service-module satellite backup

To test the hub dial backup connection for the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT), use the **service-modulesatellitebackup** command in privileged EXEC mode.

service module satellite *slot/unit* **backup** {**initiate** | **terminate**}

Syntax Description

slot	Router chassis slot in which the network module is installed.
unit	Interface number. For NM-1VSAT-GILAT network modules, always use 0.
initiate	Initiates a hub dial backup connection.
terminate	Terminates a hub dial backup connection.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The **service-modulesatellitebackup** command is used only when you configure *hub* dial backup for the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT).

Normally, the hub dial backup connection comes up only when the satellite link goes down (for example, because of a rain-fade event). The **service-modulesatellitebackup** command allows you to artificially bring down the satellite link to test the hub dial backup connection.

Examples

The following example shows how to initiate a satellite backup test:

```
Router# service-module satellite 1/0 backup initiate
```

The following example shows how to terminate a running satellite backup test:

```
Router# service-module satellite 1/0 backup terminate
```

Related Commands

Command	Description
service-module backup interface	Specifies the interface to use to back up the satellite interface on the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT).
service-module backup mode	Sets the terrestrial backup mode for the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT).

service-module satellite configuration

To enter satellite initial configuration mode, use the **service-modulesatelliteconfiguration**command in user EXEC or privileged EXEC mode.

service-module satellite *slot/unit* **configuration**

Syntax Description

slot	Router chassis slot in which the network module is installed.
unit	Interface number. For NM-1VSAT-GILAT network modules, always use 0.

Command Default

No default behavior or values.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

You need a password from your satellite service provider to enter satellite initial configuration mode.

The parameters that you configure in satellite initial configuration mode are saved directly to the network module and do not appear in the router configuration, even though you configure the parameters through the Cisco IOS CLI.

To view the parameter values that were configured in satellite initial configuration mode, use one of the following commands:

- **show** command in satellite initial configuration mode
- **service-module satellite** *slot* **/0** **status** command in privileged EXEC mode

Note This command is typically used by an installation technician. Do not use this command unless your satellite service provider instructs you to perform the satellite initial configuration and provides all necessary parameter values.

Examples

The following example shows how to enter satellite initial configuration mode:

```
Router> service-module satellite 1/0 configuration
Password: <mypassword>
Reminder:changing any parameters will result in a software reset of the module.
Router(sat-init-config)>
```

Related Commands

Command	Description
end (satellite initial configuration)	Exits satellite initial configuration mode, saves any new or changed parameters, and resets the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT).
exit (satellite initial configuration)	Exits satellite initial configuration mode, saves any new or changed parameters, and resets the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT).
service-module satellite status	Displays status information related to the hardware and software on the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT), including the initial configuration parameters.
show (satellite initial configuration)	Displays the initial configuration parameters for the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT).

service-module satellite cw-mode

To enable or disable continuous wave mode, use the **service-modulesatellitecw-mode** command in satellite interface configuration mode.

service-module satellite *slot/unit* **cw-mode** {**off** | **on frequency** *frequency* [**time** *time*]}

Syntax Description

slot	Router chassis slot in which the network module is installed.
unit	Interface number. For NM-1VSAT-GILAT network modules, always use 0.
off	Disables continuous wave mode.
on	Enables continuous wave mode.
frequency *frequency*	Frequency, in kilohertz, in the range from 900000 to 1650000.
time *time*	Length of time, in seconds, that continuous wave mode is enabled. The *time* argument is a number in the range from 60 to 1800.

Command Default

Continuous wave mode is disabled.

If the time is not specified, continuous wave mode continues until turned off.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(2)T	A password challenge was added to the command-line interface when continuous wave mode is enabled.

Usage Guidelines

Continuous wave mode can be enabled only when the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT) is in boot mode.

When continuous wave mode is enabled, the NM-1VSAT-GILAT network module transmits unmodulated carrier waves that can be used for dish antenna orientation adjustments and for signal quality measurements.

Note This command is typically used by an installation technician. Do not use this command unless your satellite service provider instructs you to do so.

Note You need a password from your satellite service provider to enable continuous wave mode.

Examples

The following example shows how to enable continuous wave mode for 2 minutes, at 900000 kilohertz:

```
Router# service-module satellite 1/0 cw-mode on frequency 900000 time 120

Password: <mypassword>
CW mode obtained.
```

The following example shows how to disable continuous wave mode:

```
Router# service-module satellite 1/0 cw-mode off

CW mode released.
```

The following example shows the message that appears when you try to enable continuous wave mode while the NM-1VSAT-GILAT network module is *not* in boot mode:

```
Router# service-module satellite 1/0 cw-mode on frequency 900000 time 120

Password <mypassword>
% CW mode NOT obtained!  Valid during boot mode only.
```

service-module satellite status

To display status information related to the hardware and software on the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT), including the initial configuration parameters, use the**service-modulesatellitestatus** command in privileged EXEC mode.

service-module satellite *slot/unit* **status** [**log**]

Syntax Description

slot	Router chassis slot in which the network module is installed.
unit	Interface number. For NM-1VSAT-GILAT network modules, always use 0.
log	Extends the output to include the last ring of messages from the firmware and the last crash dump available from the NM-1VSAT-GILAT network module.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Use the **service-modulesatellitestatus** command to troubleshoot the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT).

Examples

See the table below for **service-modulesatellitestatus** command output field descriptions.

This section provides the following examples:

Normal Operation Example

The following example shows that the link to the hub (backbone status) is up, as is expected in normal working conditions:

```
Router# service-module satellite 2/0 status

Getting status from the satellite module, please wait..
Software Versions, OS:14.2.2, RSP:1.5.1.3, MBC:1.0.0.5
HW Version:00008100
CPA Number:6204, HPS CPA:1, HSP Link:2
AA Group: 258, SW Group: 512, Download: YES
Service Module Uptime:00:06:40, Router Uptime:1 day, 20 hours, 26 minutes
Current router clocktime:*03:11:22.641 UTC Tue Dec 2 2003
Oper Mode:OPERATIONAL
, In Dial Backup:NO, Standby:NO, One-Way:NO
RBCP Received Packets:44, RBCP Sent Packets:41
Bit Error Rate:0e-0, Signal to Noise Ratio:12.4453
IP Address/Mask:10.22.1.1/255.255.255.252
Service Module MAC:00:A0:AC:00:20:60
RX Lock:LOCKED, Sync Lock:LOCKED
```

```
BackBone Status:UP
, Two-Way Mode:YES, DA/RA Mode:RA
Outbound Modulation Type:DVB, OB Code Rate:3/4
Outbound Unicast Packets:61, OB Multicast Packets:23547
Outbound ID:2, OB PID:514, OB Freq:1201000, OB Bit Rate:30000000
Outbound Sync IP address: 172.22.0.3
Inbound Start Freq:1201176, IB Stop Freq:1209336
Inbound Data Rate:307200, IB Freq Offset:0
Inbound Packets:3553
BackBone Hub Link Status:UP
BackBone Received Packets:1, BB Sent:3552
BackBone Received Retransmitted:0, BB Sent Retrans:0
Service Module Eth RX:3550, TX:47110
Service Module Eth Multicast RX:1, Multicast TX:23563
Bufs Configured:5000, Bufs Free:4951
Internal Software State parameters:
   Service Module SW State Var:3
   General IOS FSM:LINK_UP, HSRP FSM:ACTIVE, HSRP VSAT Mode:ACTIVE
   Lost Beats Total:0, Lost Beats This Retry:0
VOIP DA calls:
  NONE
```

Boot Mode Example

The following example shows that the NM-1VSAT-GILAT network module is in boot mode after a software reset, so that the link to the hub (backbone status) is down:

```
Router# service-module satellite 1/0 status

Getting status from the satellite module, please wait..
Software Versions, OS:0.0.0, RSP:1.0.0.5, MBC:0.0.0.0
HW Version:001D1757
CPA Number:6204, HPS CPA:0, HSP Link:2
AA Group: 258, SW Group: 512, Download: YES
Service Module Uptime:00:00:14, Router Uptime:1 day, 20 hours, 19 minutes
Current router clocktime:*03:04:38.017 UTC Tue Dec 2 2003
Oper Mode:BOOT
, In Dial Backup:NO, Standby:NO, One-Way:NO
RBCP Received Packets:1, RBCP Sent Packets:8
Bit Error Rate:0e-0, Signal to Noise Ratio:12.4453
IP Address/Mask:172.27.1.54/255.255.255.252
Service Module MAC:00:A0:AC:00:20:60
RX Lock:LOCKED, Sync Lock:NOT LOCKED
BackBone Status:DOWN
, Two-Way Mode:YES, DA/RA Mode:RA
Outbound Modulation Type:DVB, OB Code Rate:3/4
Outbound Unicast Packets:0, OB Multicast Packets:0
Outbound ID:2, OB PID:514, OB Freq:1201000, OB Bit Rate:30000000
Outbound Sync IP address: 172.22.0.3
Inbound Start Freq:1201176, IB Stop Freq:1209336
Inbound Data Rate:307200, IB Freq Offset:0
COUNTERS OMITTED.  Not available at this time.
Internal Software State parameters:
   Service Module SW State Var:3
   General IOS FSM:LINK_DOWN, HSRP FSM:ACTIVE, HSRP VSAT Mode:ACTIVE
   Lost Beats Total:0, Lost Beats This Retry:0
VOIP DA calls:
  NONE
```

Software Reset Example

The following example shows what appears during the beginning stages of a software reset:

```
Router# service-module satellite 2/0 status

   Getting status from the satellite module, please wait..
   % Satellite2/0 card is busy.  Status is not available.  Try later.
```

Hub Dial Backup Example

The following example shows that the hub dial backup link is being used instead of the satellite link. Note, however, that hub dial backup keeps the backbone status up. In hub dial backup mode, the NM-1VSAT-GILAT network module connects to the hub over a specified dial backup link and maintains TCP connections.

```
Router# service-module satellite 1/0 status

Getting status from the satellite module, please wait..
Software Versions, OS:14.2.3, RSP:1.5.1.3, MBC:1.0.0.5
HW Version:00008100
CPA Number:3201, HPS CPA:1, HSP Link:2
AA Group: 258, SW Group: 512, Download: YES
Service Module Uptime:02:09:38, Router Uptime:2 hours, 10 minutes
Current router clocktime:*19:28:20.195 UTC Wed Apr 7 2004
Oper Mode:OPERATIONAL, In Dial Backup:YES
, Standby:NO, One-Way:NO
RBCP Received Packets:31511, RBCP Sent Packets:31358
Bit Error Rate:0e-0, Signal to Noise Ratio:12.4453
IP Address/Mask:10.0.0.100/255.255.255.0
Service Module MAC:00:A0:AC:00:20:66
RX Lock:LOCKED, Sync Lock:NOT LOCKED
BackBone Status:UP
, Two-Way Mode:YES, DA/RA Mode:RA
Outbound Modulation Type:DVB, OB Code Rate:3/4
Outbound Unicast Packets:39944, OB Multicast Packets:45612
Outbound ID:2, OB PID:514, OB Freq:1201000, OB Bit Rate:30000000
Outbound Sync IP address: 172.22.0.3
Inbound Start Freq:1201176, IB Stop Freq:1209336
Inbound Data Rate:307200, IB Freq Offset:0
Inbound Packets:8281
BackBone Hub Link Status:UP
BackBone Received Packets:37894, BB Sent:39162
BackBone Received Retransmitted:1, BB Sent Retrans:12
Service Module Eth RX:37840, TX:129000
Service Module Eth Multicast RX:202, Multicast TX:45970
Bufs Configured:5000, Bufs Free:4949
Internal Software State parameters:
   Service Module SW State Var:3
   General IOS FSM:LINK_UP, HSRP FSM:N/A, HSRP VSAT Mode:N/A
   Lost Beats Total:0, Lost Beats This Retry:0
```

VoIP Example

The following example shows the status of VoIP calls. Note that dedicated access (DA) mode is in use, and you can see the bandwidth (26 kilobits per second) being used on the DA channels.

```
Router# service-module satellite 1/0 status

Getting status from the satellite module, please wait..
Software Versions, OS:14.2.3, RSP:1.5.1.3, MBC:1.0.0.5
HW Version:00008100
CPA Number:6202, HPS CPA:1, HSP Link:2
AA Group: 258, SW Group: 512, Download: YES
Service Module Uptime:00:34:53, Router Uptime:2 days, 21 hours, 23 minutes
Current router clocktime:*08:33:51.301 UTC Mon Feb 16 2004
Oper Mode:OPERATIONAL, In Dial Backup:NO, Standby:NO, One-Way:NO
RBCP Received Packets:335, RBCP Sent Packets:332
Bit Error Rate:0e-0, Signal to Noise Ratio:12.4453
IP Address/Mask:10.2.0.2/255.255.0.0
Service Module MAC:00:A0:AC:00:20:67
RX Lock:LOCKED, Sync Lock:LOCKED
BackBone Status:UP, Two-Way Mode:YES, DA/RA Mode:DA

Outbound Modulation Type:DVB, OB Code Rate:3/4
Outbound Unicast Packets:758, OB Multicast Packets:139823
Outbound ID:2, OB PID:514, OB Freq:1201000, OB Bit Rate:30000000
Outbound Sync IP address: 172.22.0.3
Inbound Start Freq:1201176, IB Stop Freq:1209336
Inbound Data Rate:307200, IB Freq Offset:0
Inbound Packets:346
BackBone Hub Link Status:UP
BackBone Received Packets:335, BB Sent:288
BackBone Received Retransmitted:0, BB Sent Retrans:0
Service Module Eth RX:356, TX:280163
Service Module Eth Multicast RX:1, Multicast TX:139918
Bufs Configured:5000, Bufs Free:4951
Internal Software State parameters:
   Service Module SW State Var:3
   General IOS FSM:LINK_UP, HSRP FSM:N/A, HSRP VSAT Mode:N/A
   Lost Beats Total:0, Lost Beats This Retry:0
VOIP DA calls:

   Call ID  BW (kb)
  Dst Port  Src Port  Dest Addr
  ========  ======= ========  ========  ==============
     16075      26
     18310     16866  162.0.0.2
```

Firmware Debug Log Example

The following example includes the firmware debug message log:

```
Router# service-module satellite 1/0 status log

Getting status from the satellite module, please wait..
Software Versions, OS:14.2.3, RSP:1.5.1.3, MBC:1.0.0.5
HW Version:00008100
CPA Number:1203, HPS CPA:1, HSP Link:2
AA Group: 258, SW Group: 512, Download: YES
Service Module Uptime:19:01:32, Router Uptime:1 week, 4 days, 16 hours,
15 minutes
Current router clocktime:*15:12:45.310 UTC Mon May 13 2002
Oper Mode:OPERATIONAL, In Dial Backup:NO, Standby:NO, One-Way:NO
RBCP Received Packets:9279, RBCP Sent Packets:9276
Bit Error Rate:0e-0, Signal to Noise Ratio:12.4453
IP Address/Mask:14.0.0.6/255.255.255.0
```

```
Service Module MAC:00:A0:AC:00:20:72
RX Lock:LOCKED, Sync Lock:LOCKED
BackBone Status:UP, Two-Way Mode:YES, DA/RA Mode:RA
Outbound Modulation Type:DVB, OB Code Rate:3/4
Outbound Unicast Packets:11099797, OB Multicast Packets:429401
Outbound ID:2, OB PID:514, OB Freq:1201000, OB Bit Rate:30000000
Outbound Sync IP address: 172.22.0.3
Inbound Start Freq:1201176, IB Stop Freq:1209336
Inbound Data Rate:307200, IB Freq Offset:0
Inbound Packets:674619
BackBone Hub Link Status:UP
BackBone Received Packets:11084921, BB Sent:93899
BackBone Received Retransmitted:352, BB Sent Retrans:2
Service Module Eth RX:10001424, TX:18532485
Service Module Eth Multicast RX:2615, Multicast TX:431486
Bufs Configured:5000, Bufs Free:1240
Internal Software State parameters:
   Service Module SW State Var:3
   General IOS FSM:LINK_UP, HSRP FSM:N/A, HSRP VSAT Mode:N/A
   Lost Beats Total:4, Lost Beats This Retry:0
VOIP DA calls:
  NONE
Last forced reset log from card
===============================
bb 01 e3 a3 28 00 00 10 00 01 ff 6f f0 00 00 10
00 00 2a aa 00 4f f9 5f c4 00 00 01 2a ff ff ff
ff 00 00 80 00 01 ff 6f f0 00 00 00 00 01 ff 76
b0 01 e3 a3 28 00 00 90 02 00 00 00 00 00 00 00
13 00 18 84 1c 00 00 00 00 01 e3 a3 28 00 2b 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 2b 00 00 01 ff 76 b0 00 2a a2 80 00 00 88
88 00 00 90 02 00 0a 7f 58 00 00 00 00 00 00 00
00 40 00 00 43 20 00 00 00 00 00 00 00 01 ff 76
b0 00 00 00 00 01 ff 70 20 ff ff ff
```

The table below describes the significant fields shown in the displays.

Table 28: service-module satellite status Field Descriptions

Field	Description
Software Versions HW Version	Software (not Cisco IOS) and hardware versions on the NM-1VSAT-GILAT network module. Useful for technical support.
CPA Number HPS CPA HSP Link AA Group SW Group Download	VSAT-to-hub link parameters.
Oper Mode	Operational mode; one of the following values: • OPERATIONAL--Boot complete and running operational code. • BOOT HOLD--Held in boot mode. • BOOT--In boot mode after a reset. • IDLE--Transitional state. • UNKNOWN--Indicates an error.

Field	Description
In Dial Backup	YES indicates that the satellite link is down and that the hub dial backup connection is in use. NO means that the hub dial backup connection is not in use or not configured. **Note** This field does not indicate whether *router* dial backup mode is in use.
Standby	YES indicates that the router in which the NM-1VSAT-GILAT network module is installed is in standby mode for Hot Standby Router Protocol (HSRP). NO indicates that the router in which the NM-1VSAT-GILAT network module is installed is either in active mode for HSRP, or HSRP is not configured.
One-Way	YES indicates one-way operational mode. NO indicates two-way operational mode.
RBCP Received Packets RBCP Sent Packets	Number of sent and received Router Blade Configuration Protocol (RBCP) packets.
IP Address/Mask	IP address and subnet mask of the NM-1VSAT-GILAT network module.
RX Lock Sync Lock	Corresponds to the following LEDs on the NM-1VSAT-GILAT network module faceplate: • RX LOCK--Indicates whether or not the DVB (outbound) receiver is locked. • SYNC--Indicates whether or not the NM-1VSAT-GILAT network module is synchronized with the hub timing. For both fields: • LOCKED indicates that the initial connection to the hub was successful. This means that the dish antenna is positioned correctly and the satellite initial configuration parameters are valid. • NOT LOCKED indicates that the NM-1VSAT-GILAT network module is in a transitional state during the boot process. If NOT LOCKED does not eventually become LOCKED, then the satellite initial configuration parameters are incorrect, there is a hardware problem, or the satellite signal has faded because of rain-fade or obstruction.
BackBone Status	Backbone link to the hub, either fully established (UP) or not fully established (DOWN). Corresponds to the ON LINE LED on the NM-1VSAT-GILAT network module faceplate.

Field	Description
Two-Way Mode	YES indicates two-way operational mode. NO indicates one-way operational mode.
DA/RA Mode	Indicates whether the satellite link is operating in random access (RA) or dedicated access (DA) mode. DA mode is required for VoIP calls.
Outbound Modulation Type OB Code Rate Outbound ID OB PID OB Freq OB Bit Rate Outbound Sync IP address	Satellite initial configuration parameters: • Outbound modulation type • Outbound Viterbi code rate • Outbound VSAT ID • Outbound packet identifier (PID) • Outbound frequency • Outbound data rate • Outbound synchronization IP address
Internal Software State parameters	Internal states that are useful for technical support.
VOIP DA calls	Information about VoIP calls, which use DA mode. **Note** This field appears only on routers that run VoIP-enabled Cisco IOS software images.
Last forced reset log from card	Debug information used by technical support.

Related Commands

Command	Description
show (satellite initial configuration)	Displays the initial configuration parameters for the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT).
show controllers satellite	Displays controller information about the internal router interface that connects to an installed Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT).
show interfaces satellite	Displays general interface settings and traffic rates for the internal router interface that connects to an installed Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT).

service-module service-engine

To enter the Cisco Unity Express command environment using a network module (NM) or an advanced Integration Module (AIM) card module, use the **service-moduleservice-engine** command in privileged EXEC mode.

service-module service-engine *slot/port* **session**

Syntax Description

slot	Slot number of the NM or AIM.
port	Port number of the NM or AIM.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(15)ZJ	This command was introduced for NMs.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(7)T	Support was added for AIMs.

Usage Guidelines

This command may only be used for NMs and AIMs running Cisco Unity Express. If your system does not have this hardware, then you will be unable to enter this command.

The **no** form of this command (**nointerfaceservice-engine**) is not available. You can enter the **exit** command to return to the router.

Examples

The following example shows the command for enabling Cisco Unity Express command environment using either a NM or AIM located in slot 4, port 0:

```
Router# service-module service-engine 4/0 session
Router# Trying 172.18.106.66, 2129 ... Open
```

service-module sm default-boot

To configure the SM-SRE service module to use the default BIOS and bootloader, use the **service-modulesmdefault-boot** command in privileged EXEC mode.

service-module sm *slot*/*port* **default-boot**

Syntax Description

slot	Router slot in which the service module is installed. Range: 1 to 4.
/ *port*	Port number of the module interface. Always use 0. The slash mark (/) is required.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

After a downtime event or failed upgrade, use this command to configure the service module to use the primary BIOS and primary bootloader to perform startup routines.

Examples

The following is sample output for a service module:

```
Router# service-module sm 1/0 default-boot
clear  Clear Default Boot
set    Set Default Boot

Router# service-module sm 1/0 default-boot clear
Router# service-module sm 1/0 default-boot set
```

service-module sm heartbeat-reset

To prevent Cisco IOS software from rebooting the SM-SRE service module when the heartbeat is lost, use the **service-modulesmheartbeat-reset** command in privileged EXEC mode.

service-module sm *slot/port* **heartbeat-reset** {**disable** | **enable**}

Syntax Description

slot	Number of the router slot in which the service module is installed. Range: 1 to 4.
/ *port*	Port number of the module interface. Always use 0. The slash mark (/) is required.
disable	Disables reset of the service module if the heartbeat is lost.
enable	Enables reset of the service module if the heartbeat is lost.

Command Default

Service module is reset when heartbeat is lost.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

When the service module is booted in failsafe mode or is undergoing an upgrade, this command prevents a reboot during the process.

When the service module heartbeat is lost, the router applies a fail-open or fail-close configuration option to the module, stops sending traffic to the module, and sets the module to error state. The router performs a hardware reset on the service module and monitors it until the heartbeat is reestablished.

Examples

The following example shows how to disable the service module from being reset if the heartbeat is lost:

```
Router# service-module sm 1/0 heartbeat-reset disable
```

You can display the status of the heartbeat reset feature with the **service-modulesmstatus**command:

```
Router# service-module sm 1/0 status

Service Module is Cisco IDS-Sensor 1/0
Service Module supports session via TTY line 194
Service Module heartbeat-reset is enabled <=====
```

Related Commands

Command	Description
interface sm	Configures an interface for a service module and enters interface configuration mode.
service-module sm reload	Performs a graceful shutdown and reboot of the service module.

Command	Description
service-module sm reset	Resets the service module hardware.
service-module sm shutdown	Performs a graceful shutdown of the service module.
service-module sm status	Displays configuration information related to the hardware and software on a service module.

service-module sm install

To use Cisco SRE to install an application on a service module (Cisco SM-SRE), use the **service-modulesminstall**command in privileged EXEC configuration mode.

service-module sm *slot/port* **install url** *url* [**script** *filename*] [**argument** *"string"*] [**force**]

Syntax Description

slot / port	Location of the services engine module in the router. For service modules, the slot number is 1 to 4 and the port number must be 0.
url *url*	Address of FTP or HTTP server, as defined in RFC 2396, on which application packages and Tcl scripts are located.
script	(Optional) Changes name of Tcl script to be run from default value to script specified by *filename* argument.
filename	Name of Tcl script.
argument	(Optional) Installer will not present options for the variable specified in the *string* argument.
string	Alphanumeric characters of variable to be passed directly to the Tcl script via the command line. Variable must be enclosed in quotation marks (“ ”)
force	(Optional) Tcl script automatically proceeds with install without prompting for user input.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

This command uses a common module-dependent bootloader on Cisco SRE to install a Linux-based application, such as Cisco Unity Express or Cisco AXP, on a service module (Cisco SM-SRE).

The slash mark (/) is required between the *slot* argument and the *port* argument.

You can only issue one instance of this command at a time on a router. You cannot use this command to install an application on two or more services engine modules in the same router at a time.

The Tcl script to be run must reside in the same FTP or HTTP server and directory as the application packages to be installed. If a credential is required, the user name and password must be imbedded in the url as shown in the following example:

```
Router# service-module sm 1/0 install url ftp://username:passwd@server.com/axp
```

If two or more of the optional keyword/argument combinations are used with this command, they must be issued in the order presented in the command syntax. For example, you cannot use the **force** keyword before the **script** or**argument** keywords nor the **argument** keyword before the **script** keyword when you issue this command.

Use the **script***filename* keyword/argument combination with this command to specify that the Cisco IOS software use some Tcl script other than the default installer during the installation.

Use the **argument"***string***"** keyword/argument combination with this command to manually provide variables during installation process and bypass the user interaction feature of the installer. The variable must include the left and right quotation marks (" ").

Use the **force** keyword with this command to install an application without prompting for user input. If you use this keyword and if the application requires you to provide certain variables during the installation, you should also use the **argument"***string***"** keyword/argument combination to manually provide the required variables because the **force** keyword will direct the installer to bypass all user interaction during the installation.

To stop the install while the Tcl script is being downloaded, use the **service-modulesminstallabort** command. This command cannot be used once the actual installation begins.

Examples

The following example shows how to use this command to run a "help.sre" Tcl script rather than the default installation Tcl script:

```
Router# service-module sm 1/0 install url ftp://server.com/cue script help.sre
Router#
```

The following example shows how to direct the installer to use the specified language variable for US English instead of prompting you with language options for Cisco Unity Express:

```
Router# service-module sm 1/0 install url ftp://server.com/cue argument "lang=en_us"
Router#
```

The following example shows the messages displayed on the module console during a successful installation using Cisco SRE:

```
Feb  6 19:09:22.526 EDT: %SM_INSTALL-6-INST_PROG: Service-Module-SM 1/0 PROGRESSING:
Validating package signature ...1 .
Feb  6 19:09:23.058 EDT: %SM_INSTALL-6-INST_PROG: Service-Module-SM 1/0 PROGRESSING: Parsing
 package manifest files ...1 .
Feb  6 19:09:44.742 EDT: %SM_INSTALL-6-INST_PROG: Service-Module-SM 1/0 PROGRESSING: Starting
 payload download1 .
Feb  6 19:09:52.022 EDT: %SM_INSTALL-6-INST_PROG: Service-Module-SM 1/0 PROGRESSING:
Performing Hot install ...1 .
Install successful on Service-Module-SM 1/0 Feb  6 19:10:28.826 EDT: %SM_INSTALL-6-INST_SUCC:
 Service-Module-SM 1/0 SUCCESS: install-completed .
```

Related Commands

Command	Description
service-module sm install abort	Stops the install and returns to the boot-loader prompt.
service-module sm uninstall	Uses Cisco SRE to uninstall an SRE-supported application on an SRE-enabled services engine module.

service-module sm install abort

To abort the Cisco SRE install process on a Cisco SM-SRE, use the **service-modulesminstallabort**command in privileged EXEC configuration mode.

service-module sm *slot/port* **install abort** [**force**]

Syntax Description

slot/port	Location of the services engine module in the router. For service modules, the slot number is 1 to 4 and the port number must be 0.
force	(Optional) Tcl script automatically stops the installation without prompting for confirmation.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

This command stops the installation during the downloading portion of the process only and returns the console to the boot-loader prompt. You cannot use this command to stop the process once the actual installation has begun.

Use the **force** keyword with this command to stop the process without first prompting for confirmation.

Examples

The following example shows how to use this command to stop an application installation without first prompting for confirmation:

```
Router# service-module sm 4/0 install abort force
.
.
.
boot-loader>
```

Related Commands

Command	Description
service-module sm install	Uses Cisco SRE to install an SRE-supported application on an SRE-enabled services engine module.

service-module sm reload

To perform a graceful shutdown and reboot of the SM-SRE service module operating system, use the **service-modulesmreload** command in privileged EXEC mode.

service-module **sm** *slot*/*port* **reload**

Syntax Description

slot	Router slot in which the service module is installed. Range: 1 to 4.
/ *port*	Port number of the module interface. Always use 0. The slash mark (/) is required.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

At the confirmation prompt, press **Enter** to confirm the action or **n** to cancel.

Examples

The following example shows how to gracefully shut down the module and reboot the operating system:

```
Router# service-module sm 1/0 reload

Do you want to proceed with reload?[confirm]
```

Related Commands

Command	Description
interface sm	Configures an interface for a service module and enters interface configuration mode.
service-module sm reset	Resets the service module hardware.
service-module sm shutdown	Gracefully shuts down the service module.
show diag	Displays controller information for service modules.
show interfaces sm	Displays basic interface configuration information for service modules.

service-module sm reset

To reset the SM-SRE service module hardware, use the **service-modulesmreset** command in privileged EXEC mode.

service-module sm *slot/port* **reset**

Syntax Description

slot	Router slot in which the service module is installed. Range: 1 to 4.
/ *port*	Port number of the module interface. Always use 0. The slash mark (/) is required.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

At the confirmation prompt, press **Enter** to confirm the action or **n** to cancel.

Caution Because you may lose data, use the **service-modulesmreset** command only to recover from a shutdown or failed state.

Examples

The following example shows how to reset the service module hardware:

```
Router# service-module sm 1/0 reset

Use reset only to recover from shutdown or failed state
Warning: May lose data on the the NVRAM, nonvolatile file system or unsaved configuration!
Do you want to reset?[confirm]
```

Related Commands

Command	Description
interface sm	Configures an interface for a service module and enters interface configuration mode.
service-module sm reload	Performs a graceful shutdown and reboot of the service module operating system.
service-module sm shutdown	Gracefully shuts down the service module.
show diag	Displays controller information for service modules.
show interfaces sm	Displays basic interface configuration information for service modules.

service-module sm session

To begin a configuration session for an SM-SRE service module through a console connection, use the **service-modulesmsession** command in privileged EXEC mode.

service-module sm *slot/port* **session** [**clear**]

Syntax Description

slot	Router slot in which the service module is installed. Range: 1 to 4.
/ *port*	Port number of the module interface. Always use 0. The slash mark (/) is required.
clear	(Optional) Clears the service module configuration session.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

Only one session at a time is allowed into the service module from the service module interface.

After starting a session, you can perform any service module configuration task. You first access the service module console in a user-level shell. To access the privileged EXEC command shell, where most commands are available, use the **enable** command.

After you finish configuration tasks and exit the service module console session, use this command with the **clear** keyword to clear the session. At the confirmation prompt, press **Enter** to confirm the action or **n** to cancel.

Examples

The following example shows a session being opened for an SM-SRE:

```
Router# service-module sm 1/0 session

Trying 10.10.10.1, 2129 ... Open

SE-Module con now available
Press RETURN to get started!

SE-Module> enable
```

The following example clears the session that had been used to configure the SM-SRE in slot 1:

```
Router# service-module sm 1/0 session clear
[confirm]
 [OK]
```

Related Commands

Command	Description
enable	Enters privileged EXEC mode.

Command	Description
interface	Configures an interface and enters interface configuration mode.
show diag	Displays controller information for a service module.
show interface sm	Displays basic interface configuration information for service modules.

service-module sm shutdown

To gracefully shut down an SM-SRE service module, use the **service-modulesmshutdown** command in privileged EXEC mode.

service-module sm *slot*/*port* **shutdown**

Syntax Description

slot	Router slot in which the service module is installed. Range: 1 to 4.
/ *port*	Port number of the module interface. Always use 0. The slash mark (/) is required.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

At the confirmation prompt, press **Enter** to confirm the action or **n** to cancel.

This command brings down the operating system of the specified service module in an orderly fashion to protect the hard drive. When the system is shut down, the module can be removed from the router.

Examples

The following example shows how to gracefully shut down the service module:

```
Router# service-module sm 1/0 shutdown

Do you want to proceed with shutdown?[confirm]
Use service module reset command to recover from shutdown.

WARNING: Confirm that the service-module status shows 'is Shutdown' before removing the
module or powering off the system !
```

Related Commands

Command	Description
interface sm	Configures an interface for an SM-SRE and enters interface configuration mode.
service-module sm reload	Performs a graceful shut down and reboot of the SM-SRE operating system.
service-module sm reset	Resets the hardware on the SM-SRE.
show diag	Displays controller information for service modules.
show interfaces sm	Displays basic interface configuration information for SM-SREs.

service-module sm statistics

To display reset and reload information for an SM-SRE service module and its Cisco IOS software, use the **service-modulesmstatistics**command in EXEC mode.

service-module sm *slot/port* **statistics**

Syntax Description

slot	Router slot in which the service module is installed. Range: 1 to 4.
/ *port*	Port number of the module interface. Always use 0. The slash mark (/) is required.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Examples

The following example displays information for a service module in slot 1:

```
Router# service-module sm 1/0 statistics

Module Reset Statistics:
 CLI reset count = 0
 CLI reload count = 0
 Registration request timeout reset count = 1
 Error recovery timeout reset count = 1
 Module registration count = 1
```

Related Commands

Command	Description
interface sm	Configures an interface for an SM-SRE and enters interface configuration mode.
service-module sm reload	Performs a graceful shutdown and reboot of the SM-SRE operating system.
service-module sm reset	Resets the SM-SRE hardware.
service-module sm shutdown	Gracefully shuts down the SM-SRE.
show interfaces sm	Displays basic interface configuration information for SM-SREs.

service-module sm status

To display configuration information related to the hardware and software on an SM-SRE service module, use the **service-modulesmstatus**command in privileged EXEC mode.

service-module sm *slot*/*port* **status**

Syntax Description

slot	Router slot in which the service module is installed. Range: 1 to 4.
/ *port*	Port number of the module interface. Always use 0. The slash mark (/) is required.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

Use this command to:

- Display the SM-SREs software release version
- Check the SM-SRE status (steady or down)
- Display hardware information for the SM-SRE, including CPU, memory, and interface information

Examples

The following example displays information for an SM-SRE:

```
Router# service-module sm 1/0 status

Service Module is Cisco SM1/0
Service Module supports session via TTY line 67
Service Module is in Steady state
Service Module heartbeat-reset is enabled
Getting status from the Service Module, please wait..
Cisco Foundation Software 1.0
FNDN Running on SM
No install/uninstall in progress
```

Related Commands

Command	Description
interface sm	Configures an interface for an SM-SRE and enters interface configuration mode.
show diag	Displays controller information for service modules.
show interfaces sm	Displays basic interface configuration information for SM-SREs.

service-module sm uninstall

To use Cisco SRE to uninstall an application on a service module (Cisco SM-SRE), use the **service-modulesmuninstall**command in privileged EXEC configuration mode.

service-module sm *slot/port* **uninstall** [**force**]

Syntax Description

slot / *port*	Location of the services engine module in the router. For service modules, the slot number is 1 to 4 and port number must be 0.
force	(Optional) Tcl script automatically proceeds with uninstall without prompting for confirmation.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

This command completely erases the disk or compact flash of the SRE-enabled services engine module and removes the application keys. It does not remove application licenses.

The slash mark (/) is required between the *slot* argument and the *port* argument.

You can only issue one instance of this command at a time on a router. You cannot use this command to uninstall an application on two or more services engine modules in a router at a time.

Use the **force** keyword with this command to uninstall an appliction without first prompting for confirmation.

Examples

The following example shows how to use this command to uninstall an application without first prompting for confirmation:

```
Router# service-module
 sm uninstall 1/0 force
Router#
```

Related Commands

Command	Description
service-module sm install	Uses Cisco SRE to install an SRE-supported application on an SRE-enabled services engine module.

service-module t1 cablelength short

To set transmission attenuation for shorter cable lengths, use the **service-modulet1cablelengthshort** command in interface configuration mode. To disable transmission attenuation for shorter cable lengths, use the **no** form of this command.

service-module t1 cablelength short {**110ft** | **220ft** | **330ft** | **440ft** | **550ft** | **660ft**}
no service-module t1 cablelength short

Syntax Description

110ft	Sets a cable length from 0 to 110 feet.
220ft	Sets a cable length from 111 to 220 feet.
330ft	Sets a cable length from 221 to 330 feet.
440ft	Sets a cable length from 331 to 440 feet.
550ft	Sets a cable length from 441 to 550 feet.
660ft	Sets a cable length from 551 to 660 feet.

Command Default

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
12.2(15)ZL	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.

Usage Guidelines

This command is intended only for the Version 2 card, WIC-1-DSU-T1 V2, as part of the **service-modulet1** configuration options.

Use this command to configure the transmission (tx) attenuation for cables whose length is shorter than or equal to 660 feet. The related command, **service-modulet1lbo**, is used to define the line-build-out values for cable lengths longer than 660ft. At any time, only one, either the short configuration or the lbo configuration, can exist. They cannot co-exist. The configuration of one command will cause the effect of the other command to cease and only the new command will be in effect.

Examples

The following example shows how to set the short cablelength to 220 feet.

```
Router(config)# interface serial 0/0
Router(config-if)# service-module t1 cablelength short 220ft
```

Related Commands

Command	Description
service-module t1 lbo	Configures the CSU line-build-out (lbo) on a fractional T1/T1 DSU/CSU module.

service-module t1 clock source

To specify the clock source for the fractional T1/T1 CSU/DSU module, use the **service-modulet1clocksource** command in interface configuration mode. To return to the default line clock, use the **no** form of this command.

service-module t1 clock source {**internal** | **line**}
no service-module t1 clock source

Syntax Description

internal	Specifies the CSU/DSU internal clock.
line	Specifies the line clock. This is the default.

Command Default

Line clock

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example sets an internal clock source on serial line 0:

```
Router(config)# interface serial 0
Router(config
-if)
# service-module t1 clock source internal
```

Related Commands

Command	Description
service-module 56k clock source	Sets up the clock source on a serial interface for a 4-wire, 56/64-kbps CSU/DSU module.

service-module t1 data-coding

To guarantee the ones density requirement on an alternate mark inversion (AMI) line using the fractional T1/T1 module, use the **service-modulet1data-coding**command in interface configuration mode. To enable normal data transmission, use the**no**form of this command.

service-module t1 data-coding {**inverted** | **normal**}
no service-module t1 data-coding

Syntax Description

inverted	Inverts bit codes by changing all 1 bits to 0 bits and all 0 bits to 1 bits.
normal	Requests that no bit codes be inverted before transmission. This is the default.

Command Default

Normal transmission

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Data inversion is used to guarantee the ones density requirement on an AMI line when using bit-oriented protocols such as High-Level Data Link Control (HDLC), PPP, X.25, and Frame Relay. If the time slot speed is set to 56 kbps, this command is rejected because line density is guaranteed when transmitting at 56 kbps. Use this command with the 64-kbps line speed.

If you transmit inverted bit codes, both CSU/DSUs must have this command configured for successful communication.

Examples

The following example inverts bit codes using a time slot speed of 64 kbps:

```
Router(config)# interface serial 0
Router(config
-if)
# service-module t1 timeslots all speed 64
Router(config
-if)
# service-module t1 data-coding inverted
```

Related Commands

Command	Description
service-module t1 linecode	Selects the linecode for the fractional T1/T1 module.
service-module t1 timeslots	Defines time slots that constitute a fractional T1/T1 (FT1/T1) channel.

service-module t1 fdl

To set the facilities data link (FDL) parameter to either ATT or ANSI, use the**service-modulet1fdl** command in interface configuration mode. To ignore the FDL parameter, use the **no** form of this command.

service-module t1 fdl {**ansi** | **att**}
no service-module t1 fdl

Syntax Description

ansi	Sets the FDL parameter to ANSI.
att	Sets the FDL parameter to ATT.

Command Default

Determined by the telephone company

Command Modes

Interface configuration

Command History

Release	Modification
11.2 P	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The default is **noservice-modulet1fdl**. The **ansi** or **att** options are determined by your service provider or telephone company.

Examples

The following example sets the FDL parameter to ANSI:

```
Router(config)# interface serial 0
Router(config
-if)
# service-module t1 fdl ansi
```

service-module t1 framing

To select the frame type for a line using the fractional T1/T1 (FT1/T1) module, use the **service-modulet1framing** command in interface configuration mode. To revert to the default, Extended Super Frame, use the **no**form of this command.

service-module t1 framing commandservice-module t1 framing {**esf** | **sf**}
no service-module t1 framing commandservice-module t1 framing {**esf** | **sf**}

Syntax Description

esf	Specifies extended super frame (ESF) as the T1 frame type. This is the default.
sf	Specifies D4 super frame (SF) as the T1 frame type.

Command Default

esf

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command in configurations in which the router communicates with FT1/T1 data lines. The service provider determines which framing type, either **esf** or **sf**, is required for your circuit.

Examples

The following example enables Super Frame as the FT1/T1 frame type:

```
Router(config
-if)
# service-module t1 framing sf
```

service-module t1 lbo

To configure the CSU line-build-out (LBO) on a fractional T1/T1 CSU/DSU module, use the **service-modulet1lbo**command in interface configuration mode. To disable line-build-out, use the **no**form of this command.

service-module t1 lbo {**-15 db** | **-7.5 db** | **none**}
no service-module t1 lbo {**-15 db** | **-7.5 db** | **none**}

Syntax Description

-15 db	Decreases outgoing signal strength by 15 dB.
-7.5 db	Decreases outgoing signal strength by 7.5 dB.
none	Transmits packets without decreasing outgoing signal strength.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to decrease the outgoing signal strength to an optimum value for a fractional T1 line receiver. The ideal signal strength should be -15 dB to -22 dB, which is calculated by adding the phone company loss, cable length loss, and line build out.

You may use this command in back-to-back configurations, but it is not needed on most actual T1 lines.

Examples

The following example sets the LBO to -7.5 dB:

```
Router(config)# interface serial 0
Router(config
-if)
# service-module t1 lbo -7.5 db
```

service-module t1 linecode through show controllers satellite

service-module t1 linecode

To select the line code for the fractional T1/T1 module, use the **service-modulet1linecode**command in interface configuration mode. To select the default, the B8ZS line code, use the**no** form of this command.

service-module t1 linecode {**ami** | **b8zs**}
no service-module t1 linecode {**ami** | **b8zs**}

Syntax Description

ami	Specifies alternate mark inversion (AMI) as the line code.
b8zs	Specifies binary 8 zero substitution (B8ZS) as the line code. This is the default.

Command Default

The default line code is B8ZS.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Configuring B8ZS is a method of ensuring the ones density requirement on a T1 line by substituting intentional bipolar violations in bit positions four and seven for a sequence of eight zero bits. When the CSU/DSU is configured for AMI, you must guarantee the ones density requirement in your router configuration using the **service-modulet1data-codinginverted** command or the **service-modulet1timeslotsspeed56**command.

Your T1 service provider determines which line code, either **ami**or **b8zs**, is required for your T1 circuit.

Examples

The following example specifies AMI as the line code:

```
Router(config)# interface serial 0
Router(config
-if)
# service-module t1 linecode ami
```

Related Commands

Command	Description
service-module t1 data-coding	Guarantees the ones density requirement on an AMI line using the fractional T1/T1 module.
service-module t1 timeslots	Defines time slots that constitute a fractional T1/T1 (FT1/T1) channel.

service-module t1 remote-alarm-enable

To generate remote alarms (yellow alarms) at the local CSU/DSU or detect remote alarms sent from the remote CSU/DSU, use the **service-modulet1remote-alarm-enable**command in interface configuration mode. To disable remote alarms, use the**no** form of this command.

service-module t1 remote-alarm-enable
no service-module t1 remote-alarm-enable

Syntax Description

This command has no arguments or keywords.

Command Default

Remote alarms are disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Remote alarms are transmitted by the CSU/DSU when it detects an alarm condition, such as a red alarm (loss of frame) or blue alarm (unframed ones). The receiving CSU/DSU then knows that there is an error condition on the line.

With D4 Super Frame configured, a remote alarm condition is transmitted by setting the bit 2 of each time slot to zero. For received user data that has the bit 2 of each time slot set to zero, the CSU/DSU interprets the data as a remote alarm and interrupts data transmission, which explains why remote alarms are disabled by default. With Extended Super Frame configured, the remote alarm condition is signalled out of band in the facilities data link.

You can see if the FT1/T1 CSU/DSU is receiving a remote alarm (yellow alarm) by issuing the **showservice-moduleserial** command.

Examples

The following example enables remote alarm generation and detection:

```
Router(config)# interface serial 0
Router(config
-if)
# service-module t1 remote-alarm-enable
```

Related Commands

Command	Description
service-module t1 framing	Selects the frame type for a line using the fractional T1/T1 (FT1/T1) module.
show service-module serial	Displays performance statistics for an integrated CSU/DSU.

service-module t1 remote-loopback

To specify that the fractional T1/T1 DSU/CSU module enters loopback mode when it receives a loopback code on the line, use the **service-modulet1remote-loopback** command in interface configuration mode. To disable remote loopbacks, use the **no** form of this command.

service-module t1 remote-loopback {**full** | **payload v54**}
no service-module t1 remote-loopback {**full** | **payload v54**}

Syntax Description

full	Configures the remote loopback code used to transmit or accept CSU loopback requests.
payload	Configures the loopback code used by the local CSU/DSU to generate or detect payload-loopback commands.
v54	Industry standard loopback code. Use this keyword for CSU/DSUs that may not support the Accunet loopup standards. This keyword is used only with a payload request, not a full request.

Use the **full**keyword to enable the standard loopup codes, which use a 1-in-5 pattern for loopup and a 1-in-3 pattern for loopdown. Use the **payloadv54**keywords to enable the v54 pseudo-random loopup codes for loopup and v54 pseudo-random loopdown codes for loopdown.

Command Default

Full and payload loopbacks with standard loopup codes

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.3(2)T	The provision for an **alternate** loopback code was removed.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **no** form of this command disables loopback requests. For example, the **noservice-modulet1remote-loopbackfull** command ignores all full-bandwidth loopback transmissions and requests.

Configuring the **no** form of the command might not prevent telco line providers from looping your router in extended super frame (esf) mode because fractional T1/T1 lines use facilities data link messages to initiate loopbacks.

To have the loopback remote commands on the FT1/T1 CSU/DSU module function successfully, you need to enable the **service-modulet1remote-loopback** command.

Note Use the **full**keyword to enable the standard loopup codes, which use a 1-in-5 pattern for loopup and a 1-in-3 pattern for loopdown. Use the **payloadv54**keywords to enable the v54 pseudorandom codes for loopup and v54 pseudorandom codes for loopdown.

Examples

The following example shows how to configure two routers connected back-to-back through a fractional T1/T1 line to enter loopback mode:

```
Router(config)# interface serial 0/0
Router(config-if)# service-module t1 remote-loopback full

Router(config-if)# loopback remote full
!
%SERVICE_MODULE-5-LOOPUPREMOTE: Unit Serial0/0 - Remote unit placed in loopback
Router(config-if)# no loopback remote
%SERVICE_MODULE-5-LOOPDOWNREMOTE: Unit Serial0/0 - Remote loopback test cancelled
The following example shows how to configure two routers connected back-to-back through a
fractional T1/T1 line to enter loopback mode and generate or detect payload-loopback commands:
Router(config-if)# service-module t1 remote-loopback payload v54

Router(config-if)# loopback remote payload
%%SERVICE_MODULE-5-LOOPUPREMOTE: Unit Serial0/0 - Remote unit placed in loopback
```

Related Commands

Command	Description
loopback remote (interface)	Loops packets through a DSU/CSU to a remote DSU/CSU and back over a channelized T1 link.

service-module t1 timeslots

To define time slots that constitute a fractional T1/T1 (FT1/T1) channel , use the **service-modulet1timeslots**command in interface configuration mode. To resume the default setting (all FT1/T1 time slots transmit at 64 kbps), use the **no** form of this command.

service-module t1 timeslots {*range* | **all**} [**speed** {**56** | **64**}]
no service-module t1 timeslots {*range* | **all**}

Syntax Description

range	The DS0 time slots that constitute the FT1/T1 channel. The range is from 1 to 24, where the first time slot is numbered 1 and the last time slot is numbered 24. Specify this field by using a series of subranges separated by commas.
all	Selects all FT1/T1 time slots.
speed	(Optional) Specifies the time slot speed.
56	(Optional) 56 kbps.
64	(Optional) 64 kbps. This is the default.

Command Default

64 kbps is the default for all time slots.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command specifies which time slots are used in fractional T1 operation and determines the amount of bandwidth available to the router in each FT1/T1 channel.

The time-slot range must match the time slots assigned to the channel group. Your service provider defines the time slots that comprise a channel group.

To use the entire T1 line, enable the **service-modulet1timeslotsall**command.

Examples

The following example displays a series of time-slot ranges and a speed of 64 kbps:

```
Router(config
-if)
# service-module t1 timeslots 1-10,15-20,22 speed 64
```

Related Commands

Command	Description
service-module t1 data-coding	Guarantees the ones density requirement on an AMI line using the fractional T1/T1 module.
service-module t1 linecode	Selects the linecode for the fractional T1/T1 module.

service-module wlan-ap bootimage

To configure the boot image on the service module, use the **service-module wlan-ap bootimage** command in privileged EXEC mode.

service-module wlan-ap *interface number* **bootimage** [{**autonomous** | **unified**}]

Syntax Description

interface number	The interface number for the wireless device. Always use 0.
autonomous	Autonomous software image.
unified	Upgrade image with Lightweight Access Point Protocol (LWAPP).

Command Default

Autonomous software image

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(20) T	This command was introduced for wireless-enabled Cisco 880 Series and Cisco 890 Series Integrated Services Routers.

Usage Guidelines

When running the advanced IP services feature set on either Cisco 880 Series routers or Cisco 890 Series routers, use the **service-module wlan-ap 0 bootimage unified command**to enable the Cisco unified software upgrade image on the embedded wireless access point. After enabling the unified image, use the **service-module wlan-ap 0 reload** command to perform a graceful shutdown and reboot of the access point.

Note The **service-module wlan-ap 0 bootimage**command does not support recovery images on the embedded access point. Use the **service-module wlan-ap 0 reload** command to shutdown and reboot the access point.

Cisco 880 Series and Cisco 890 Series routers with embedded access point running the unified software image require DHCP to obtain an IP address for the access point. An IP address is needed to communicate with the Wireless LAN Controller (WLC) and to download its image upon boot up. The host router can provide DHCP server functionality through the DHCP pool to reach the WLC, and setup option 43 for the controller IP address in the DHCP pool configuration.

Use the following guideline to setup a DHCP pool on the host router.

```
ip dhcp pool embedded-ap-pool
    network 60.0.0.0 255.255.255.0
    default router 60.0.0.1
    option 43 hex f104.0a0a.0a0f  /* Single WLC IP address (10.10.10.15) in HEX format */
int vlan 1  /* Default Vlan */
ip address 60.0.0.1 255.255.255.0
int Wlan-GigabitEthernet0 /* internal switch-port to AP */
switchport access vlan 1
```

Examples

The following example upgrades the embedded access point image from autonomous to unified.

```
Router#configure terminal
Router(config)#service-module wlan-ap 0 bootimage unified
 *Jan 18 05:31:58.172: %WLAN_AP_SM-6-UNIFIED_IMAGE: Embedded AP will change boot image to
mini-IOS also called LWAPP recovery Please check router config to ensure connectivity between
 WLC and AP. Use service-module wlan-ap 0 reload to bootup mini-IOS image on AP
Router(config)#end
Router#
*Jan 18 05:32:04.136: %SYS-5-CONFIG_I: Configured from console by console
Router#service-module wlan-ap 0 reload
 Reload will save AP config....
Do you want to proceed with reload?[confirm] Trying to reload Service Module wlan-ap0.
Router#
Service Module saved config, start reset.
Received reload request from router
Saving configuration...
Building configuration...
```

Related Commands

Command	Description
interface wlan-ap	Enters wireless interface configuration mode to configure an interface.
service-module wlan-ap reload	Performs a graceful shutdown and reboot of the service module.
service-module wlan-ap reset	Resets the service module hardware.

service-module wlan-ap reload

To perform a graceful shutdown and reboot of the service module use the **service-module wlan-ap reload** command in privileged EXEC mode.

service-module wlan-ap *interface number* **reload**

Syntax Description

interface number	The interface number for the wireless device. Always use 0.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(20)T	This command was introduced for wireless-enabled Cisco 860, 880, and 890 Integrated Services Routers.

Usage Guidelines

Autonomous Mode

At the confirmation prompt, press **Enter** to confirm the action, or press **n** to cancel.

Note When running in autonomous mode, the reload command saves the configuration before rebooting. If the attempt is unsuccessful, the following message displays: Failed to save service module configuration.

Unified Mode

The service module reload command is usually handled by the Wireless LAN Controller (WLC).

Note When running in Unified mode, the reload command will produce the following message: The embedded wireless device is in Unified mode. Reload/reset is normally handled by WLC controller. Still want to proceed? [yes]

Examples

The following examples show a graceful shut down and reboot of the service module:

Autonomous Mode

```
Router# service-module wlan-ap0 reload
Do you want to proceed with reload?[confirm]
Router# reload
Do you want to reload the internal AP ? [yes/no]:
Do you want to save the configuration of the AP ? [yes/no]:
System configuration has been modified. Save [yes/no]:
Proceed with reload? [confirm]
```

Unified Mode

```
Router# service-module wlan-ap0 reload
The embedded AP is in Unified mode. Reload/reset is normally handled by WLC controller.
Still want to proceed? [yes]
Router# reload
The embedded AP is in Unified mode. Reload/reset is normally handled by WLC controller.
Do you want to reload the internal AP [yes/no]:
System configuration has been modified. Save [yes/no]:
Proceed with reload [Confirm]
```

Related Commands

Command	Description
interface wlan-ap	Enters wireless interface configuration mode to configure an interface.
service-module wlan-ap reset	Resets the service module hardware.

service-module wlan-ap reset

To reset the service module hardware, software, and configuration, use the **service-module wlan-ap reset** command in privileged EXEC mode.

service-module wlan-ap interface number reset [{**bootloader** | **default-config**}]

Syntax Description

interface number	The interface number for the wireless device. Always use 0.
bootloader	Resets the wireless device to the bootloader for manual image recovery.
default-config	Resets the wireless device to the factory default configuration.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(20)T	This command was introduced for wireless-enabled Cisco 860, 880, and 890 Integrated Services Routers.

Usage Guidelines

At the confirmation prompt, press **Enter** to confirm the action, or press **n** to cancel.

Caution Because you may lose data, use the **service-module wlan-ap reset** command only to recover from a shutdown or failed state.

Examples

The following example resets a wireless device on a router that is operating in either autonomous mode or LWAPP mode:

Autonomous Mode

```
Router# service-module wlan-ap0 reset
Use reset only to recover from shutdown or failed state.
```

LWAPP Mode

```
Router# service-module wlan-ap0 reset
The embedded device is in LWAPP mode. Reload/reset is normally handled by WLC controller.
Still want to proceed? [yes]
```

Resetting the Factory Default Configuration on the Wireless Device

The following example resets the wireless device to the default configuration.

```
Router#service-module wlan-ap 0 reset default-config
Router#
```

Recovering the Image on the Wireless Device

The following example resets the wireless device down to the bootloader level for manual image recovery.

```
Router#service-module wlan-ap0 reset bootloader
Router#
```

Related Commands

Command	Description
interface wlan-ap	Enters wireless interface configuration mode to configure an interface.
service-module wlan-ap reload	Performs a graceful shutdown and reboot of the service module.

service-module wlan-ap session

To begin a configuration session with a service module through a console connection use the **service-module wlan-ap session** command in privileged EXEC mode.

service-module wlan-ap *interface number* **session** [{**clear** | **disconnect**}]

Syntax Description

interface number	The interface number for the wireless device. Always use 0.
clear	(Optional) Clears the wireless device configuration session.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(20)T	This command was introduced for wireless-enabled Cisco 860, 880, and 890 Integrated Services Routers.

Usage Guidelines

Only one session is allowed at a time into the wireless device from a router console-port connection. After starting a session, perform configuration tasks on the wireless device. You first access the router in a user-level shell. To access the privileged EXEC command shell, where most commands are available, use the **enable** command.

When you finish configuring the device, and would like to exit the console session, type Ctrl-Shift 6x to return to the router's console. Type service-module wlan-ap session **clear** or disconnect to close the session with the device. At the confirmation prompt, press **Enter twice**to confirm the action or **n** to cancel.

Note If you do not clear or disconnect the session on the service module, it will remain open in the background after you return to the router's console prompt. When the session is open in the background, pressing Enter will toggle you back to the wireless device prompt.

Examples

The following example shows a session being opened on a service-module in an ISR:

```
Router# service-module wlan-ap 0 session
Trying 1.2.3.4, 2002 ... Open
AP#
```

The following example clears the session on the service-module in the ISR:

```
Router#service-module wlan-ap 0 session clear
[confirm]
 [OK]
```

Related Commands

Command	Description
enable	Enters privileged EXEC mode.
interface wlan-ap	Enters wireless interface configuration mode to configure an interface.

service-module wlan-ap statistics

To display reset and reload information for a service module and its operating system software, use the **service-module wlan-ap statistics**command in privileged EXEC mode.

service-module wlan-ap interface number statistics

Syntax Description

interface number	The interface number for the wireless device. Always use 0.

Command Default

none

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(20)T	This command was introduced for wireless-enabled Cisco 860, 880, and 890 Integrated Services Routers.

Examples

The following example displays information for wireless-enabled Cisco ISRs:

```
Router#service-module wlan-ap 0 statistics
Module Reset Statistics:
  CLI reset count = 0
  CLI reload count = 1
  Registration request timeout reset count = 0
  Error recovery timeout reset count = 0
  Module registration count = 10
The last IOS initiated event was a cli reload at *04:27:32.041 UTC Fri Mar 8 2007
```

Related Commands

Command	Description
interface wlan-ap	Enters wireless interface configuration mode and configures a wireless device.
service-module wlan-ap reset	Resets the wireless device.
service-module wlan-ap reload	Performs a graceful shutdown and reboot on the wireless device.

service-module wlan-ap status

To display configuration information related to hardware and software on the service module, use the **service-module wlan-ap status**command in privileged EXEC mode.

service-module wlan-ap *interface number* **status**

Syntax Description

interface number	The interface number for the wireless device. Aways use 0.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(20)T	This command was introduced for wireless-enabled Cisco 860, 880, and 890 Integrated Services Routers.

Usage Guidelines

Use the **service-module wlan-ap status** command to

- Display the wireless device’s software release version
- Check the wireless device’s status (steady or down)
- Display hardware information for the wireless device, including image, memory, interface, and system uptime

Examples

The following example displays information for the wireless device on a Cisco Integrated Services Router:

```
Router#service-module wlan-ap 0 status

Service Module is Cisco wlan-ap0
Service Module supports session via TTY line 2
Service Module is in Steady state
Service Module reset on error is disabled
Getting status from the Service Module, please wait..
Image path = flash:c8xx_19xx_ap-k9w7-mx.acregr/c8xx_19xx_ap-k9w7-mx.acre
gr
System uptime = 0 days, 4 hours, 28 minutes, 5 seconds
Router#d was introduced for embedded wireless LAN access points on Cisco 860 and 880 Series
 Integrated Services Routers.
```

Related Commands

Command	Description
interface wlan-ap	Enters wireless service module's console interface.

session slot

To open a session with a module (for example, the Multilayer Switch Module (MSM), Network Analysis Module (NAM), or Asynchronous Transfer Mode (ATM)), use the **sessionslot** command in EXEC mode.

session slot *mod* **processor** *processor-id*

Syntax Description

mod	Slot number.
processor *processor-id*	Specifies the processor ID.

Command Default

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

To end the session, enter the **quit** command.

This command allows you to use the module-specific CLI.

Examples

This example shows how to open a session with an MSM (module 4):

```
Router# session slot 4 processor 2
Router#
```

set ip df

To change the Don't Fragment (DF) bit value in the IP header, use the **setipdf** command in route-map configuration mode. To disable changing the DF bit value, use the **no** form of this command.

set ip df {**0** | **1**}
no set ip df {**0** | **1**}

Syntax Description

0	Sets the DF bit to 0 (clears the DF bit) and allows packet fragmentation.
1	Sets the DF bit to 1 which prohibits packet fragmentation.

Command Default

The DF bit value is not changed in the IP header.

Command Modes

Route-map configuration

Command History

Release	Modification
12.1(6)	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Using Path MTU Discovery (PMTUD) you can determine an MTU value for IP packets that avoids fragmentation. If ICMP messages are blocked by a router, the path MTU is broken and packets with the DF bit set are discarded. Use the **setipdf** command to clear the DF bit and allow the packet to be fragmented and sent. Fragmentation can slow the speed of packet forwarding on the network but access lists can be used to limit the number of packets on which the DF bit will be cleared.

Note Some IP transmitters (notably some versions of Linux) may set the identification field in the IP header (IPid) to zero when the DF bit is set. If the router should clear the DF bit on such a packet and if that packet should subsequently be fragmented, then the IP receiver will probably be unable to correctly reassemble the original IP packet.

Examples

The following example shows how to clear the DF bit to allow fragmentation. In this example a router is blocking ICMP messages and breaking the path MTU. Using policy routing both the inbound and outbound packets on interface serial 0 will have their DF bit set to 0 which allows fragmentation.

```
interface serial 0
ip policy route-map clear-df-bit
route-map clear-df-bit permit 10
match ip address 111
set ip df 0
access-list 111 permit tcp any any
```

Related Commands

Command	Description
ip tcp path-mtu-discovery	Enables Path MTU Discovery.
route-map	Defines a route map to control where packets are output.

set platform hardware qfp active feature ipsec event-monitor

To set the threshold for IP Security (IPsec) crypto failure, use the **set platform hardware qfp active feature ipsec event-monitor type <*failure type*> count** command in the user EXEC mode. To reset the IPsec crypto failure threshold, use the **clear** form of this command.

set platform hardware qfp active feature ipsec event-monitor type {**decrypt failed** | **encrypt failed** | **replay**} **count** *value*

clear set platform hardware qfp active feature ipsec event-monitor type {**decrypt failed** | **encrypt failed** | **replay**} **count value**

Syntax Description

type	Sets the type of event monitor failure. The following options are available: • *decrypt failed* • *encrypt failed* • *replay*
count	Sets the monitored event threshold count.
value	The value of the monitored event threshold count. The range is from 1 to 4294967295. The default value is 0.

Command Default

The event monitor is not enabled.

Command Modes

User EXEC (#)

Command History

Release	Modification
Cisco IOS 12.2 XN	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

The following example shows how to set the threshold for IPsec crypto failure:

```
Device> set platform hardware qfp active feature ipsec event-monitor type replay count 1
```

shdsl annex

To define the single-pair high-bit-rate digital subscriber line (SHDSL) G.991.2 standard, use the **shdslannex**command in config controller DSL group mode.

shdsl annex {*annexstandard*}

Syntax Description

standard	Defines the standard for the selected type of DSL group. The following annex standards are supported: • A • A-B-F-G • A-F • B (Default annexure) • B-G • F • G **IMA Group** • A • A-B • B **M-PAIR Group** • A • A-B • B • F {coding 16 | 32} • F-G {coding 16 | 32} • G {coding 16 | 32} **1-PAIR and 2-PAIR Group** • A • A-B • B • F {coding 16 | 32} • F-G {coding 16 | 32} • G {coding 16 | 32}

Command Default

SHDSL annex B

Command Modes

Config controller DSL group

Command History

Release	Modification
12.4(15)T	This command was introduced for the Cisco HWIC-4SHDSL and HWIC-2SHDSL running on the Cisco 1841 router and on the Cisco 2800 and 3800 series access routers.
15.1(1)T	This command was modified. The argument *annex* was introduced for the Cisco HWIC-4SHDSL-E

Usage Guidelines

Use the dsl-group command to create a DSL group, and then use the shdsl annex command to define the G.991.2 standard for the DSL group.

Examples

The following example uses the shdsl annex command to define the annex standard for a 2-Pair DSL group on a Cisco HWIC-4SHDSL:

```
Router(config-controller-dsl-group)# shdsl annex ?
  A    Annex A of G.991.2 standard
  A-B  Annex A/B of G.991.2 standard
  B    Annex B of G.991.2 standard
  F    Annex F of G.991.2 standard
  F-G  Annex F/G of G.991.2 standard
  G    Annex G of G.991.2 standard
Router(config-controller-dsl-group)# shdsl annex g ?
  coding  16-TCPAM or 32-TCPAM line coding
Router(config-controller-dsl-group)# shdsl annex g coding ?
  16-TCPAM  16-TCPAM line coding
  32-TCPAM  32-TCPAM line coding
Router(config-controller-dsl-group)# shdsl annex g coding 16 ?
  <cr>
```

Example

```
Router(config-controller-dsl-group)#shdsl annex ?
  A        Annex A of G.991.2 standard
  A-B-F-G  Annex A/B/F/G of G.991.2 standard
  A-F      Annex A/F of G.991.2 standard
  B        Annex B of G.991.2 standard
  B-G      Annex B/G of G.991.2 standard
  F        Annex F of G.991.2 standard
  G        Annex G of G.991.2 standard
Router(config-controller-dsl-group)#shdsl annex f ?
coding  16-TCPAM, 32-TCPAM line coding or auto-TCPAM line coding
```

The above TCPAM configurations are valid only in case the termination is "co". In case the termination is CPE, user will see the following output

```
Router(config-controller-dsl-group)#shdsl annex f ?
<cr>
```

Related Commands

Command	Description
dsl-group	Creates a DSL group and enters config controller DSL group mode.
shdsl rate	Defines the SHDSL rate.

shdsl rate

To define the single-pair high-bit-rate digital subscriber line (SHDSL) rate, use the **shdslrate**command in config-controller-dsl-group mode.

shdsl rate {*number* | **auto**}

Syntax Description

number	SHDSL rate for the digital subscriber line (DSL) group. **DSL Group with 1 Pair** Annex A & B--192-2304 kbps Annex F & G (32 TC-PAM)--768-5696 kbps Annex F & G (16 TC-PAM)--2304-3840 kbps **DSL Group with 2 Pairs** Annex A & B--384-4608 kbps Annex F & G (32 TC-PAM)--1536-11392 kbps Annex F & G (16 TC-PAM)-- 4608-7680 kbps **DSL Group with 3 Pairs** Annex A & B--576-6912 kbps Annex F & G (32 TC-PAM)--2304-12288 kbps Annex F & G (16 TC-PAM)-- 6912-11520 kbps **DSL Group with 4 Pairs** Annex A & B--768-9216 kbps Annex F & G (32 TC-PAM)--3072-16384 kbps Annex F & G (16 TC-PAM)-- 9216-15360 kbps

	Data rates supported for each Annex and TC-PAM 2-wire configuration. For EFM bonding configuration with multiple links, multiply the data rate ranges by the number of links in the EFM bonding group. **2-wire, 16-TCPAM** Annex A--192 - 2304 kbps Annex B--192 - 2304 kbps Annex F--2304 - 3840 kbps Annex G--2304 - 3840 kbps Annex A & F--192 - 3840 kbps Annex B & G--192 - 3840 kbps A & B & F & G--192 - 3840 kbps **2-wire, 32-TCPAM** Annex F--768 - 5696 kbps Annex G--768 - 5696 kbps Annex A & F--768 - 5696 kbps Annex B & G--768 - 5696 kbps Annex A & B & F & G--768 - 5696 kbps **2-wire Auto-TCPAM** Annex A--192 - 2304 kbps Annex B--192 - 2304 kbps Annex F--768 - 5696 kbps Annex G--768 - 5696 kbps Annex A & F--192 - 5696 kbps Annex B & G--192 - 5696 kbps Annex A & B & F & G--192 - 5696 kbps
auto	Sets this SHDSL rate to automatic mode.

Command Default

The command default is the maximum annex rate for the selected DSL group.

Command Modes

Config controller DSL group

Command History

Release	Modification
12.4(15)T	This command was introduced for the Cisco HWIC-4SHDSL and HWIC-2SHDSL running on the Cisco 1841 router and on the Cisco 2800 and 3800 series access routers.
15.1(1)T	This command was modified. Support for the for the Cisco HWIC-4SHDSL-E is added.

Usage Guidelines

Use the dsl-group command to create a DSL group, and then use the shdsl annex command to define the G.991.2 standard for the newly created DSL group. Define the SHDSL line rate with the shdsl rate command.

Examples

The following example defines the SHDSL line rate for DSL group 1, pairs 0-1 (2 pairs) on a Cisco HWIC-4SHDSL:

```
Router(config-controller)# dsl-group 1 pairs 0-1 ima
Router(config-controller-dsl-group)#
Sep 22 14:53:46.481: %HWIC_SHDSL-5-DSLGROUP_UPDOWN: SHDSL 0/2/0 dsl-group(1) state changed
 to down.
Sep 22 14:53:48.481: %LINK-3-UPDOWN: Interface ATM0/2/IMA1, changed state to down
Sep 22 14:53:49.481: %LINEPROTO-5-UPDOWN: Line protocol on Interface ATM0/2/IMA1, changed
state to down
Router(config-controller-dsl-group)# shdsl annex ?
  A    Annex A of G.991.2 standard
  A-B  Annex A/B of G.991.2 standard
  B    Annex B of G.991.2 standard
Router(config-controller-dsl-group)# shdsl annex b ?
  <cr>
Router(config-controller-dsl-group)# shdsl rate auto
  <384-4608>  DSL Rate in kbps(line will train at the rate + 16kbps overhead)
  auto        auto rate mode
```

The following example shows adaptive rate configurations.

```
Router(config-controller-dsl-group)#shdsl rate ?
<768-9216>  DSL Rate (excluding DSL overhead) in kbps
auto        auto rate mode
Router(config-controller-dsl-group)#shdsl rate 1024
Router(config-controller-dsl-group)#shdsl rate auto ?
current  Current SNR Margin
snext    Self Near end cross talk

Router(config-controller-dsl-group)#shdsl rate auto current ?
<0 - 10>  0dB to 10dB
Router(config-controller-dsl-group)#shdsl rate auto snext ?
<-10 - 10>  -10dB to 10dB
```

Related Commands

Command	Description
dsl-group	Creates a DSL group and enters config controller DSL group mode.
shdsl annex	Defines the G.991.2 standard for a DSL group.

shelf-id

To change the shelf number assigned to the router shelf or dial shelf on the Cisco AS5800, use the **shelf-id** command in global configuration mode. To return the shelf numbers to the default value, use the **no** form of this command.

shelf-id *number* {**router-shelf** | **dial-shelf**}
no shelf-id *number*

Syntax Description

number	Number to assign to the shelf. Range is from 0 to 9999.
router-shelf	Specified number to the router shelf.
dial-shelf	Specified number to the dial shelf.

Command Default

The default shelf number for the router shelf is 0.

The default shelf number for the dial shelf is 1, or one number higher than the specified router shelf number.

Command Modes

Global configuration

Command History

Release	Modification
11.3(2)AA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The shelf number is used to distinguish between cards on the router shelf and cards on the dial shelf.

Caution You must reload the Cisco AS5800 for the shelf number to take effect. The shelf numbers are part of the interface names. When you reload the Cisco AS5800, all NVRAM interface configuration information is lost.

You can specify the shelf number through the setup facility during initial configuration of the Cisco AS5800. This is the recommended method to specify shelf numbers.

To display the shelf numbers, use the **showrunning-config** command. If a shelf number has been changed, the pending change is shown in the output of the **showversion** command (for example, the dial-shelf ID is 87; will change to 2 on reload).

Examples

In the following example, the dial shelf is assigned the number 456:

```
Router(config)# shelf-id 456 dial-shelf
Router(config)# exit
```

Related Commands

Command	Description
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

show (satellite initial configuration)

To display the initial configuration parameters for the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT), use the **show** command in satellite initial configuration mode.

show

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Satellite initial configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

This command is typically used by an installation technician. Do not use this command unless your satellite service provider instructs you to perform the satellite initial configuration and provides all necessary parameter values.

You can view the satellite initial configuration parameters by entering the **service-modulesatellite***slot*/**0status** command in privileged EXEC mode.

Examples

The following example shows the satellite initial configuration parameters for the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT):

```
Router(sat-init-config)# show

!
! Initial Configuration Parameters:
!
id aa-group 298
id software group 598
id vsat 6201
mode download
mode two-way
outbound data-pid 514
outbound data-rate 15000000
outbound frequency 1201000
outbound id 2
outbound modulation-type DVB
outbound sync ip address 172.16.0.3
outbound viterbi-rate 1/2
!
!
Router(sat-init-config)#
```

Related Commands

Command	Description
service-module satellite status	Displays status information related to the hardware and software on the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT), including the initial configuration parameters.

show alarm-interface

To display the alarm interface controller (AIC) configuration setting and the information sent to the Cisco IOS software by the AIC, use the **showalarm-interface** command in privileged EXEC mode.

show alarm-interface [*slot-number*] [**summary**]

Syntax Description

slot-number	(Optional) Slot number in which the AIC was placed.
summary	(Optional) Selects the summary format for the output message.

Command Default

Displays verbose message output and displays all AICs in all slot numbers on the router.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)XG	This command was introduced on the Cisco 2600 series and Cisco 3600 series.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Examples

The following is sample output from the **showalarm-interfacesummary** command:

```
Router# show alarm-interface 5 summary
         Alarm Interface Card in Slot 5:
Configured IP address:10.2.130.102
Status: KEEPALIVE TIMER EXPIRED
Alarm Interface Card in Slot 5:
Configured IP address:10.2.130.102
Status:KEEPALIVE TIMER EXPIRED
```

The following is an example of a verbose **showalarm-interface**display:

```
Router# show alarm-interface 4
         Alarm Interface Card in Slot 4:
Configured IP address: 10.10.10.2
Status: RUNNING
Timer expires in < 11 min.
Reported version: 00 00 00 01
Expected version: 00 00 00 01
Last Self Test result: READY
Last Start-Up message:
----------
<AIC>: Hardware Version 1, Revision A Software Version 2, Revision A 1.0.1 Installed and
running, POST passed.
----------
Last Status severity: 0
Last Status message:
----------
Status
----------
```

The table below describes significant fields shown in this output.

Table 29: show alarm-interface Field Descriptions

Field	Description
Alarm Interface Card in Slot	Card type and slot number.
Configured IP address	Configured IP address
Status	AIC card status. Can be one of the following: • HARDWARE DETECTED • RUNNING • HARDWARE NOT PRESENT • KEEPALIVE TIMER EXPIRED
Timer expires in	Current value of the KEEPALIVE TIMER, or states if the timer has been disabled. This line is only active when the status line reads HARDWARE DETECTED or RUNNING. Used in troubleshooting to detect operational failures of the AIC.
Reported version	Active software version number. Comparing the reported version to the expected version may reveal possible incompatibilities between the AIC's software and the IOS image.
Expected version	Expected software version number. Comparing the reported version to the expected version may reveal possible incompatibilities between the AIC's software and the IOS image.
Last Self Test result	Result of the AIC's power on self-test (POST).
Last Start-Up message	Startup messages.
<AIC>	AIC. Includes version and activity information.
Last Status severity	Rates the severity of the status message. Any number other than 0 indicates a need for intervention. The number 1 indicates the most severe condition.
Last Status message	Last status message.

Related Commands

Command	Description
alarm-interface	Enters the alarm interface mode and configures the AIC.

show alarm-profile

To verify the alarm profile configured for chassis, use the **show alarm-profile** command.

Syntax Description

Syntax Description:

There are no keywords.

Command Default

There is no default.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 16.8.1	Support for this command was introduced on ASR 900 Series.

Examples

```
Router# show alarm profile
Alarm profile CHASSIS:
 SONET/SDH:
  Alarm Name                          Severity   Syslog
  Section Loss of Frame Failure       CRITICAL   Enabled
  Line Alarm Indication Signal        INFO       Enabled
  Line Remote Failure Indication      INFO       Enabled
  Path Alarm Indication Signal        INFO       Enabled
  Path Remote Failure Indication      INFO       Enabled
  Path Loss of Pointer                INFO       Enabled
 DS1:
  Alarm Name                          Severity   Syslog
  Receiver has loss of signal         CRITICAL   Enabled
  Receiver has loss of frame          INFO       Enabled
  Receiver has remote alarm           INFO       Enabled
 DS3:
  Alarm Name                          Severity   Syslog
  Receiver has loss of signal         MAJOR      Enabled
  DS1 Alarm Indication Signal         MINOR      Enabled
  DS1 Loss Of Frame                   INFO       Enabled
  DS1 Remote Alarm Indication         INFO       Enabled
```

show als

To display Automatic Laser Shutdown (ALS) status, use the show als command in privileged EXEC mode.

show als {**all** | **interface** **slot**/**port**}

Syntax Description

all	Displays ALS status for all interfaces.
interface	Displays ALS status for the selected interface .
slot/port	Number of the chassis slot that contains the interface, where: • slot--Chassis slot number. • /port--Port number.

Command Default

No default behavior or values

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRD1	This command was introduced on the Cisco 7600 series routers.

Examples

The following example shows the ALS status for the selected interface:

```
Router# show als interface t2/1
TenGigabitEthernet2/1
 Mode ALS_MODE_MANUAL
 Pulse Width 100 sec
 Pulse Interval 150 sec
 Current state ALS_STATE_NORMAL

The following example shows the ALS status for all interfaces:
Router# show als all
TenGigabitEthernet2/1
 Mode ALS_MODE_MANUAL
 Pulse Width 100 sec
 Pulse Interval 150 sec
 Current state ALS_STATE_NORMAL

TenGigabitEthernet2/2
 Mode ALS_MODE_AUTOMATIC
 Pulse Width 100 sec
 Pulse Interval 300 sec
 Current state ALS_STATE_NORMAL
```

Related Commands

Command	Description
als	Enables the ALS mode.

Command	Description
als restart	Requests an ALS restart mode.
als restart mode	Selects the ALS restart mode.
als restart pulse	Select the ALS pulse mode.
hw-module als restart	Requests a restart pulse.

show aps

To display information about the current automatic protection switching (APS) feature, use the **showaps** command in privileged EXEC mode.

show aps commandshow aps

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1CC	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **showaps**command on a router configured with a working interface. In this example, POS interface 0/0/0 is configured as a working interface in group 1, and the interface is selected (that is, active).

```
Router1# show aps
POS0/0/0 working group 1 channel 1 Enabled Selected
```

The following is sample output from the **showaps**command on a router configured with a protect interface. In this example, POS interface 2/0/0 is configured as a protect interface in group 1, and the interface is not selected (the ~ indicates that the interface is not active). The output also shows that the working channel is located on the router with the IP address 10.1.6.1 and that the interface is currently selected (that is, active).

```
Router2# show aps
POS2/0/0 protect group 1 channel 0 bidirectional ~Selected
        Rx_K1= 0, Rx_K2= 0 Tx_K1= 0 Tx_K2= 5
        Working channel 1 at 10.1.6.1 Enabled
```

For the K1 field (8 bits), the first 4 bits indicate the channel number that has made the request, and the last 4 bits map to the requests (local or external) listed in the table below. For the K2 field (8 bits), the first 4 bits indicate the channel number bridged onto the protect line, the next bit is the architecture used, and the last 3 bits indicate the mode of operation or non-APS use listed in the table below.

Table 30: K1 Bit Descriptions

Bits (Hexadecimal)	Description
K1 bits 8765	K1 bits 8 through 5: Channel number that made the request.
K1 bits 4321	K1 bits 4 through 1: Type of request.

Bits (Hexadecimal)	Description
1111 (0xF)	Lockout of protection request.
1110 (0xE)	Forced switch request.
1101 (0xD)	Signal failure (SF)--high priority request.
1100 (0xC)	Signal failure (SF)--low priority request.
1011 (0xB)	Signal degradation (SD)--high priority request.
1010 (0xA)	Signal degradation (SD)--low priority request.
1001 (0x9)	Not used.
1000 (0x8)	Manual switch request.
0111 (0x7)	Not used.
0110 (0x6)	Wait to restore request.
0101 (0x5)	Not used.
0100 (0x4)	Exercised request.
0011 (0x3)	Not used.
0010 (0x2)	Reverse request.
0001 (0x1)	Do not revert request.
0000 (0x0)	No request.

show asic-version

To display the application-specific integrated circuit (ASIC) version for a specific module, use the **showasic-version** command in EXEC mode.

show asic-version slot *number*

Syntax Description

slot	The slot that the ASIC is installed in.
number	Module number.

Command Default

This command has no default settings.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Cisco 7600 series routers.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

In the **showasic-version**command output, the ASIC types are as follows:

- Lyra--Layer 2 forwarding engine
- Medusa--Crossbar and bus fabric interface
- Polaris--Layer 3 CEF engine
- Pinnacle--4-port Gigabit Ethernet interface
- Titan--Packet rewrite and replication engine
- Vela--Constellation bus interface

Examples

This example shows how to display the ASIC type and version for a specific module:

```
Router# show asic-version slot 1
Module in slot 1 has 3 type(s) of ASICs
        ASIC Name      Count      Version
        ASIC1          (2.0)
        ASIC2          (2.0)
        ASIC3 1        (0.1)
Router#
```

Related Commands

Command	Description
show module	Displays the module status and information.

show c7300

To display the types and status of cards installed in a Cisco 7304 router, use the **showc7300**command in privileged EXEC mode.

show c7300

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(9)EX	This command was introduced.
12.1(10)EX	The output of this command was enhanced to include information about Field-Programmable Gate Array (FPGA) images.
12.1(10)EX2	The output of this command was enhanced to include information about a standby route processor (RP).
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(20)S	Support was added for the Cisco 7304 router.
12.2(20)S2	Support was added for modular services cards (MSCs) and shared port adapters (SPAs) on the Cisco 7304 router.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command displays the types and status of cards installed in a Cisco 7304 router (such as network services engines [NSEs], RPs, line cards, MSCs, and SPAs), and information about incompatible FPGA images. When the bundled and current FPGA images are compatible, they are not displayed.

This command also displays whether your system is in compliance with line card configuration guidelines. For NSEs and line cards, empty slots are not displayed in the output. However, for SPAs, several status values are reported, including an empty subslot, which is reported as “missing.”

If your system contains an unsupported line card or RP with no matching bundled FPGA image in Cisco IOS software, then this command displays “None” instead of the bundled FPGA version number.

Use this command to display information about the status of the active and standby NSEs.

Examples

The following example displays information about a Cisco 7304 router that has current FPGA images:

```
Router# show c7300
Slot      Card Type           Status          Insertion time
```

```
----      ---------           ------          --------------
0,1       NSE-100             Active          00:13:16 ago
4         1OC48-POS           Active          00:01:43 ago
System is compliant with hardware configuration guidelines.
All the FPGAs in the system are up-to-date
Network IO Interrupt Throttling:
 throttle count=3, timer count=3
 active=0, configured=1
 netint usec=3999, netint mask usec=200
```

The following example displays information about a Cisco 7304 router that has incompatible FPGA images that need to be updated. If your system contains an unsupported line card or RP with no matching bundled FPGA image in Cisco IOS software, “None” is displayed instead of a bundled FPGA version number.

```
Router# show c7300
Slot      Card Type           Status          Insertion time
----      ---------           ------          --------------
0,1       NSE-100             Active          00:02:26 ago
4         6T3                 Active          00:02:23 ago
5         6T3                 Active          00:02:23 ago
System is compliant with hardware configuration guidelines.
%WARNING:The following FPGAs in the system may need an update.
Slot      Card Type           Current FPGA    Bundled FPGA
----      ---------           ------------    ------------
0         NSE-100 (MB)        0.12            None
Network IO Interrupt Throttling:
 throttle count=0, timer count=0
 active=0, configured=1
 netint usec=3999, netint mask usec=200
```

The following example displays sample output information about the redundancy status of the NSEs installed in the system. In the following example, the active RP is the NSE-100 installed in slot 0 and slot 1. The standby is the NSE-100 installed in slot 2 and slot 3.

```
Router# show c7300
Slot      Card Type           Status          Insertion time
----      ---------           ------          --------------
0,1       NSE-100             Active          00:02:03 ago
2,3       NSE-100             Standby         00:02:03 ago
4         4OC3-POS            Active          00:01:59 ago
5         6T3                 Active          00:01:59 ago
System is compliant with hardware configuration guidelines.
Network IO Interrupt Throttling:
 throttle count=0, timer count=0
 active=0, configured=1
 netint usec=3999, netint mask usec=200
```

The following example displays information about a Cisco 7304 router with an NSE-100, MSC-100s, and 4-Port 10/100 Fast Ethernet SPAs:

```
Router# show c7300
Slot      Card Type           Status          Insertion time
----      ---------           ------          --------------
0,1       NSE100              Active          00:45:29 ago
2         7304-MSC-100        Active          00:44:36 ago
3         7304-MSC-100        Active          00:44:36 ago
4         7304-MSC-100        Active          00:44:36 ago
5         7304-MSC-100        Active          00:14:39 ago
The FPGA versions for the cards listed above are current
Shared Port Adapter information:
```

```
Slot/Subslot  SPA Type          Status         Insertion time
------------  --------          ------         --------------
2/0           SPA-4FE-7304      ok             00:44:36 ago
2/1           SPA-4FE-7304      ok             00:44:36 ago
3/0           SPA-4FE-7304      ok             00:44:35 ago
3/1           not present       missing        never
4/0           SPA-4FE-7304      ok             00:44:35 ago
4/1           SPA-4FE-7304      ok             00:44:35 ago
5/0           SPA-4FE-7304      ok             00:14:36 ago
5/1           SPA-4FE-7304      ok             00:14:36 ago
Network IO Interrupt Throttling:
 throttle count=1, timer count=1
 active=0, configured=1
 netint usec=3999, netint mask usec=200
```

The table below provides a description for each of the possible status fields for SPAs.

Table 31: SPA Status Field Descriptions

Status Field for SPAs	Description
booting	SPA is initializing.
failed	SPA is powered off due to five automatic recovery failures.
FW mismatch	An FPGA version mismatch with the Cisco IOS software has been detected for the SPA.
missing	SPA is not present in the MSC subslot.
not allowed online	SPA is not supported.
ok	SPA is operational.
stopped	SPA is deactivated by the **hw-modulesubslotstop**command.
unknown	SPA is in unrecognizable state.

Related Commands

Command	Description
show c7300 errorlog	Displays error information about a Cisco 7304 router.
show diag	Displays hardware information for any slot or the chassis.
show redundancy (7300)	Displays redundancy information for the active and standby NSEs.
show version	Displays the configuration of the system hardware, the number of each interface type installed, the Cisco IOS software version, the names and sources of configuration files, and the boot images. Displays the configuration of the ROM monitor.

show c7300 errorlog

To display error information on a Cisco 7304 router running pre-Cisco IOS Release 12.2(25)S software, use the **showc7300errorlog**command in privileged EXEC mode.

show c7300 errorlog [{**slot** *slot-number* | **all**}]

Syntax Description

slot	(Optional) Displays error information for the hardware in a slot.
slot-number	(Optional) Specifies the slot location of the hardware to display error information.
all	(Optional) Displays error information for all hardware in all slots.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(9)EX	This command was introduced.
12.2(18)S	This command was introduced on Cisco 7304 routers running Cisco IOS Release 12.2 S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Each line card in a Cisco 7304 router has a serial channel connecting to the processor. There are two serial channel controllers on each serial channel, one for the line card side and one for the processor side. Each serial channel has four serial links labeled as SL0, SL1, SL2 and SL3. This command displays a set of error counters for each serial link.

Use this command to display board-level errors. If you are investigating controller or interface errors, use the **showcontroller** and**showinterface** commands.

Examples

The following example displays error information about a line card in slot 2 on a Cisco 7304 router:

```
Router# show c7300 errorlog slot 2
        Backplane serial channel controller (Santa Ana):
        LC 2, LC Santa Ana, channel A, error counters:
                              SL0  SL1  SL2  SL3
        Reframe:            [   0    0    0    0 ]
        Overrun:            [   0    0    0    0 ]
        Underrun:           [   0    0    0    0 ]
        OOB:                [   0    0    0    0 ]
        Disparity:          [   0    0    0    0 ]
        Missing_Ctrl_Code:  [   0    0    0    0 ]
        Chip access errors: [   0    0    0    0 ]
        LC 2, NSE Santa Ana 0, channel A, error counters:
                              SL0  SL1  SL2  SL3
        Reframe:            [   0    0    0    0 ]
```

```
        Overrun:            [    0    0    0    0 ]
        Underrun:           [    0    0    0    0 ]
        OOB:                [    0    0    0    0 ]
        Disparity:          [    0    0    0    0 ]
        Missing_Ctrl_Code:  [    0    0    0    0 ]
        Chip access errors: [    0    0    0    0 ]
```

The following example displays error information about all hardware in all of the slots on a Cisco 7304 router:

```
Router# show c7300 errorlog slot all
        Backplane serial channel controller (Santa Ana):
        LC 2, LC Santa Ana, channel A, error counters:
                              SL0  SL1  SL2  SL3
        Reframe:            [    0    0    0    0 ]
        Overrun:            [    0    0    0    0 ]
        Underrun:           [    0    0    0    0 ]
        OOB:                [    0    0    0    0 ]
        Disparity:          [    0    0    0    0 ]
        Missing_Ctrl_Code:  [    0    0    0    0 ]
        Chip access errors: [    0    0    0    0 ]
        LC 2, NSE Santa Ana 0, channel A, error counters:
                              SL0  SL1  SL2  SL3
        Reframe:            [    0    0    0    0 ]
        Overrun:            [    0    0    0    0 ]
        Underrun:           [    0    0    0    0 ]
        OOB:                [    0    0    0    0 ]
        Disparity:          [    0    0    0    0 ]
        Missing_Ctrl_Code:  [    0    0    0    0 ]
        Chip access errors: [    0    0    0    0 ]
        Backplane serial channel controller (Santa Ana):
        LC 3, LC Santa Ana, channel A, error counters:
                              SL0  SL1  SL2  SL3
        Reframe:            [    0    0    0    0 ]
        Overrun:            [    0    0    0    0 ]
        Underrun:           [    0    0    0    0 ]
        OOB:                [    0    0    0    0 ]
        Disparity:          [    0    0    0    0 ]
        Missing_Ctrl_Code:  [    0    0    0    0 ]
        Chip access errors: [    0    0    0    0 ]
        LC 3, NSE Santa Ana 0, channel A, error counters:
                              SL0  SL1  SL2  SL3
        Reframe:            [    0    0    0    0 ]
        Overrun:            [    0    0    0    0 ]
        Underrun:           [    0    0    0    0 ]
        OOB:                [    0    0    0    0 ]
        Disparity:          [    0    0    0    0 ]
        Missing_Ctrl_Code:  [    0    0    0    0 ]
        Chip access errors: [    0    0    0    0 ]
```

The table below describes the significant fields shown in the display.

Table 32: show c7300 errorlog Field Descriptions

Field	Description
Reframe	A data frame on a serial link does not align to the designated framing boundary.
Overrun:	Packets are stored in a FIFO buffer when the serial link is overloaded.
Underrun:	A serial link looks for packets in an empty FIFO buffer.

Field	Description
OOB:	Out of band error. An undefined serial link control character is received.
Disparity:	A running disparity error occurs on the link.
Missing_Ctrl_Code:	Missing Control Code. An incorrect number of control codes are received.
Chip access errors:	Access to the serial channel device fails.

Related Commands

Command	Description
show c7300	Displays the types of hardware currently installed in a Cisco 7304 router.
show diag	Displays hardware information for any slot or the chassis.
show platform errorlog	Displays error information.
show version	Displays the configuration of the system hardware, the number of each interface type installed, the Cisco IOS software version, the names and sources of configuration files, and the boot images. Displays the configuration of the ROM monitor.

show c7300 pxf accounting

To display the number and types of packets entering or exiting the PXF processors, use the **showc7300pxfaccounting** command in privileged EXEC mode.

show c7300 pxf accounting

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(9)EX	This command was introduced.
12.2(14)SZ	This command was modified to **showpxfaccounting** for the Cisco 7304 router. All Cisco IOS releases prior to 12.2(14)SZ that support the Cisco 7304 still require that **showc7300pxfaccounting** be entered to gather PXF accounting output.
12.2(18)S	This command was introduced on Cisco 7304 routers running Cisco IOS Release 12.2S.
12.2(20)S	The **c7300** keyword was removed. Entering **showpxfaccounting** could get the information previously gathered by entering the **showc7300pxfaccounting** command.

Usage Guidelines

Use the **showc7300pxfaccounting** command to display the number of packets entering and exiting the PXF processors.

The c7300 keyword was removed from this command in Cisco IOS Release 12.2(20)S. The**showpxfaccounting** command can be used in post-Cisco IOS Release 12.2(20)S releases to gather information previously gathered by entered the **showc7300pxfaccounting** command.

Examples

The following example displays output of the**showc7300pxfaccounting** command:

```
Router# show c7300 pxf accounting
PXF Utilization:14 %
PXF Packet Counters:
 Ingress from GE :             0      Egress to GE :             8
 Ingress from LCs:      24783520      Egress to LCs:      18387770
 Ingress from RP :            10      Egress to RP :             2
 Priority queue  :            12      Default queue:      18387787
Drop Packet Counters:
    ACL input deny Drop:        6395752
```

The table below describes the significant fields shown in the display.

Table 33: show c7300 pxf accounting Field Descriptions

Field	Description
Ingress from GE:	Packets coming into the PXF processors from the Gigabit Ethernet ports.

Field	Description
Egress to GE:	Packets going to the Gigabit Ethernet ports from the PXF processors.
Ingress from LCs	Packets coming in to the PXF processors from line card ports.
Ingress from RP	Packets coming in to the PXF processors from the Route Processor.
Drop Packet Counters:	Packets dropped by the PXF processors.
ACL input deny Drop:	Packets dropped because of the implicit deny all at the end of all ACLs.

Related Commands

Command	Description
ip pxf	Manually enables the PXF processor.
show pxf accounting	Displays the number and types of packets entering or exiting the PXF processors.
show c7300 pxf interfaces	Displays the status of various interfaces know to the PXF processors.

show c7300 pxf interfaces

Note Effective with Cisco IOS Release 12.2(20)S, the **showc7300pxfinterfaces** command is replaced by the **showpxfinterfaces** command. See the **showpxfinterfaces** command for for information.

To display the status of various interfaces known to the Parallel Express Forwarding (PXF) processors, use the **showc7300pxfinterfaces**command in privileged EXEC mode.

show c7300 pxf interfaces {*interface-index* | **all**}

Syntax Description

interface-index	A number that represents an interface known to the PXF processors. Valid values are 0 to 32767.
all	Specifies all PXF interfaces.

Command Default

No default behaviors or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(9)EX	This command was introduced.
12.2(14)SZ	This command was modified to **showpxfinterfaces** for the Cisco 7304 router. All Cisco IOS releases prior to 12.2(14)SZ that support the Cisco 7304 still require that **showc7300pxfinterfaces** be entered to gather PXF interface information.
12.2(18)S	This command was introduced on Cisco 7304 routers running Cisco IOS Release 12.2S.
12.2(20)S	This command was replaced by the show pxf interfaces command.

Examples

The following example shows how to display information about PXF interface 1:

```
Router# show c7300 pxf interfaces 1
PXF-If: 00001  Gi0/0    (Up, Punting to RP - no ip route-cache)
  Features: in=iACL  [0x11],  out=None [0x0]
```

The following example shows how to display information about all PXF interfaces:

```
Router# show c7300 pxf interfaces
 all
PXF-If: 00001  Gi0/0    (Up, Punting to RP - no ip route-cache)
  Features: in=iACL  [0x11],  out=None [0x0]
PXF-If: 00002  Gi0/1    (Down, Punting to RP - no ip route-cache)
  Features: in=None [0x1],  out=None [0x0]
PXF-If: 00007  In Use, Reserved
PXF-If: 00024  PO2/0    (Up, Punting to RP - no ip route-cache)
  Features: in=None [0x1],  out=None [0x0]
PXF-If: 00025  PO2/1    (Down, Punting to RP - no ip route-cache)
```

```
  Features: in=None [0x1],  out=None [0x0]
PXF-If: 00026  PO2/2    (Down, Punting to RP - no ip route-cache)
  Features: in=None [0x1],  out=None [0x0]
PXF-If: 00027  PO2/3    (Down, Punting to RP - no ip route-cache)
  Features: in=None [0x1],  out=None [0x0]
```

The table below describes the significant fields shown in the display.

Table 34: show c7300 pxf interfaces Field Descriptions

Field	Description
PXF-IF:	Internal PXF interface number. This is a unique number assigned by PXF.
Gi 0/0 or PO2/3	Type of interface.
Features:	Ingress and egress features on the PXF interface.
in=	Ingress features.
iACL	Input Access Control Lists is configured on this interface.
[0x11]	Hexadecimal value of features flag for input features on this interface.
out=	Egress features.
[0x0]	Hexadecimal value of feature flag for output features on this interface.
(Up, Punting to RP)	Interface status. Interface is up and packets are being sent to the Route Processor.
(Down, Punting to RP)	Interface status. Interface is down and packets are being sent to the Route Processor.
- no ip route-cache	Reason packets are being sent to the Route Processor. In this display, packets are being sent to the Route Processor because the user has entered the **noiproute-cache** command and CEF is not enabled on the interface. Entering the following commands causes packets to be sent to the Route Processor: • **no ip cef** • **no ip routing** • **no ip route-cache** Other reasons may be displayed: • lineproto down--The line is down. • unsupported feature--Packets from a feature that is not supported by PXF.

Related Commands

Command	Description
ip pxf	Manually enables the PXF processors.
show c7300 pxf accounting	Displays the number of packets entering or exiting the PXF processors.
show pxf interfaces	Displays the status of various interfaces known to the PXF processors.

show c7300 slot

To display various output useful for technical support purposes, enter the **showc7300slot**command in privileged EXEC mode.

show c7300 slot {*slot-number* | **all**}

Syntax Description

slot-number	Displays various information for the hardware in a particular slot. This information is useful for technical support purposes only.
all	Displays various information for all of the hardware in all of the router slots. This information is useful for technical support purposes only.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(20)S	This command replaces the show platform slot command.

Usage Guidelines

This command should not be used. The output gathered from this command is useful for technical support purposes only.

Examples

The following example shows how to display information about the hardware in slot 4 of Cisco 7304 router:

```
Router# show c7300 slot 4
Slot 4 Details
  Card Name: OC12-POS
  Card Present: Yes
  Slot Card Type: 0x377
  Saved Slot Card Type (Persistent after the OIR): 0x377
  Slot State (4): Activated
  Slot Previous State (4): Activated
  Slot Return (Transient) State (3): Analyzing
  Current Event to the OIR FSM: Idle (0)
  Current External Event to the OIR FSM: Idle (0)
  Slot Flags (0x100000):
    FPGA Checked
  Slot Ready: Yes
  Slot Retry Count: 0
  Slot Structure Address: 0x446FAED0
  Slot Sync Data Address : 0x446FB318
Slot 4 Line Card Plugin Details
  Line Card Type: OC12-POS (0x377)
  Number of Ports: 1
  Line Card Plugin Address: 0x45E123C0
  Line Card Compatible S/W Version: 0.0 (0x0)
  Line Card H/W Version: 02.03 (0x203)
  Line Card FPGA Version: 00.20 (0x14)
  Minimum Line Card H/W Version required by the S/W: 00.00 (0x0)
  Minimum Line Card FPGA Version required by the S/W: 00.01 (0x1)
```

```
  Slot 4 Line Card Devices:
  Line Card Common Devices
    Device#0: EEPROM
      Plugin Address 0x433BB830, C2W Control Structure Address 0x433C1138
      Card Bus (4): Address 0x50, Frequency 0x13, Slot 4
    Device#1: CPLD
      Plugin Address 0x433BF9E0, C2W Control Structure Address 0x433C1198
      Card Bus (4): Address 0x30, Frequency 0x13, Slot 4
    Device#2: FPGA Flash
      Plugin Address 0x433BFC30, C2W Control Structure Address 0x433C11F8
      Card Bus (4): Address 0x30, Frequency 0x13, Slot 4
(Output removed for readability)
```

Related Commands

Command	Description
show platform slot	Displays various output useful for technical support purposes.

show cable bundle

To display the forwarding table for the specified interface, use the **showcablebundle** command in privileged EXEC mode.

show cable bundle *bundle-number forwarding-table*

Syntax Description

bundle-number	Specifies the bundle identifier. Valid range is from 1 to 255.
forwarding-table	Displays the forwarding table for the specified interface.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

In the following example, a cable bundle of 25 is specified:

```
Router# show cable bundle 25 forwarding-table
MAC address         Interface
0050.7366.17ab      Cable3/0
0050.7366.1803      Cable3/0
0050.7366.1801      Cable3/0
```

The table below describes the significant fields shown in the display.

Table 35: show cable bundle Field Descriptions

Field	Description
MAC address	Media Access Control ID for each interface in the bundle.
Interface	The cable interface slot and port number.

Related Commands

Command	Description
cable bundle	Creates an interface bundle.

show cable-diagnostics tdr

To display the test results for the Time Domain Reflectometry (TDR) cable diagnostics, use the **showcable-diagnosticstdr**command in privileged EXEC mode.

show cable-diagnostics tdr interface *interface interface-number*

Syntax Description

interface *interface*	Specifies the interface type; valid values are**fastethernet** and **gigabitethernet**.
interface-number	Module and port number.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(17a)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXD	The output was changed as follows: • The Local Pair field was changed to the Pair field. The local pair designations were changed as follows: • Pair A to Pair 1-2 • Pair B to Pair 3-4 • Pair C to Pair 5-6 • Pair D to Pair 7-8 • The Remote Pair field was removed. • The Channel field was added to display the pair designation and are as follows: • Pair A • Pair B • Pair C • Pair D
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **showcable-diagnosticstdr** command is supported on specific modules. See the Release Notes for Cisco IOS Release 12.2 SX on the Catalyst 6500 and Cisco 7600 Supervisor Engine 720, Superivsor Engine 32, and Supervisor Engine 2 for the list of the modules that support TDR.

In the event of an open or shorted cable, the accuracy of length of where the cable is open or shorted is plus or minus 2 meters.

The pair length can be displayed in meters (m), centimeters (cm), or kilometers (km).

If the TDR test has not been run on the port, the following message is displayed:

```
TDR test was never run on Gi2/12
```

Examples

This example shows how to display the information about the TDR test:

```
Router# show cable-diagnostics tdr interface gigabitethernet 8/1
TDR test last run on: February 25 11:18:31
Interface Speed Pair Cable length        Distance to fault   Channel Pair status
--------- ----- ---- ------------------- ------------------- ------- ------------
Gi8/1     1000  1-2  1    +/- 6  m       N/A                 Pair B  Terminated
                3-4  1    +/- 6  m       N/A                 Pair A  Terminated
                5-6  1    +/- 6  m       N/A                 Pair C  Terminated
                7-8  1    +/- 6  m       N/A                 Pair D  Terminated
```

The table below describes the fields in the **showcable-diagnosticstdr**command output.

Table 36: show cable-diagnostics tdr Command Output Fields

Field	Description
Interface	Interface tested.
Speed	Current line speed.
Pair	Local pair name.
Cable Length	Cable length and accuracy. The accuracy unit is displayed in meters (m), centimeters (cm), or kilometers (km).
Channel	Pair designation.
Pair status	Pair status displayed is one of the following: • Terminated--The link is up. • Shorted--A short is detected on the cable. • Open--An opening is detected on the cable. • Not Completed--The test on the port failed. • Not Supported--The test on the port is not supported. • Broken--The pair is bad--either open or shorted. • ImpedanceMis--The impedance is mismatched. • InProgress--The diagnostic test is in progress.

Related Commands

Command	Description
clear cable-diagnostics tdr	Clears a specific interface or clear all interfaces that support TDR.
test cable-diagnostics	Tests the condition of 10-Gigabit Ethernet links or copper cables on 48-port 10/100/1000 BASE-T modules.

show card-protection CPGN detail

To verify card protection configuration, use the **show card-protection CPGN detail** command.

Syntax Description

Syntax Description:

There are no keywords.

Command Default

There is no default.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
XE Everest 16.7.1	This command was integarted into the Cisco NCS 4200 Series and Cisco ASR 900 Series.

Example:

Examples

```
#show card-protection 4 detail
Working(0/1:  ):
    Number of LOS Alarms:0
    ok,Active
    1:1, non-revertive

    Protect(0/2: ):
    Number of LOS Alarms:0
    ok,Inactive
    1:1, non-revertive

Revert Timer : (Not Started)
Last switchover reason: Serdes
```

show catalyst6000

To display the information about the chassis, use the **show catalyst6000** command in user EXEC or privileged EXEC mode.

show catalyst6000 {**all** | **chassis-mac-address** | **switching-clock** | **traffic-meter**}

Syntax Description

all	Displays the MAC-address ranges and the current and peak traffic-meter reading.
chassis-mac-address	Displays the MAC-address range.
switching-clock	Displays the failure recovery mode of the switching clock.
traffic-meter	Displays the percentage of the backplane (shared bus) utilization.

Command Default

The default is **all**

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXI	The output of the **show catalyst6000 traffic-meter** command was changed to include traffic monitor status information.

Usage Guidelines

If you enter the **switching-clock** keywords, the output displays whether switching of the redundant clock sources on the backplane is allowed if the active clock source fails.

There are either 64 or 1024 MAC addresses that are available to support the software features. You can enter the **show catalyst6000 chassis-mac-address** command to display the MAC-address range on your chassis.

In Cisco IOS Release 12.2(33)SXI and later releases, the traffic monitor status information is displayed in the output. In earlier releases, only the current and peak traffic-meter readings are displayed.

Examples

This example shows how to display the MAC-address ranges and the current and peak traffic-meter readings:

```
Router>
show catalyst6000 all
chassis MAC addresses: 64 addresses from 0001.6441.60c0 to 0001.6441.60ff
  traffic meter =   0%  Never cleared
           peak =   0%  reached at 08:14:38 UTC Wed Mar 19 2003
  switching-clock: clock switchover and system reset is allowed
Router>
```

This example shows how to display the MAC-address ranges:

```
Router#
show catalyst6000 chassis-mac-address
chassis MAC addresses: 1024 addresses from 00d0.004c.1800 to 00d0.004c.1c00
Router#
```

The following example shows how to display the current and peak traffic-meter readings and the traffic monitor status:

```
Router
>
show catalyst6000 traffic-meter
traffic meter =   0%  Never cleared
           peak =   0%        reached at 10:54:49 UTC Wed Mar 19 2008
     -----= Traffic Utilization Monitor Status ===---
            State  Interval  Threshold  MsgCount  LastMsgTime
-----------------------------------------------------------------------------
Backplane    Off      60s       80%        0     --
Fpoe#0  In   Off      60s       80%        0     --
       out   Off      60s       80%        0     --
Fpoe#1  In   Off      60s       80%        0     --
       out   Off      60s       80%        0     --
Fpoe#2  In   Off      60s       80%        0     --
       out   Off      60s       80%        0     --
Fpoe#3  In   Off      60s       80%        0     --
       out   Off      60s       80%        0     --
Fpoe#4  In   Off      60s       80%        0     --
       out   Off      60s       80%        0     --
.
.
.
Fpoe#19 In   Off      60s       80%        0     --
       out   Off      60s       80%        0     --
Router
>
```

This example shows how to display the failure recovery mode of the switching clock:

```
Router> show catalyst6000 switching-clock
switching-clock: clock switchover and system reset is allowed
Router>
```

Related Commands

Command	Description
monitor traffic-utilbackplane	Enables the backplane traffic utilization monitor or sets the traffic monitor interval.
monitor traffic-util fpoe	Sets the fabric channel traffic utilization monitor to generate SYSLOG messages.
show environment alarm	Displays the information about the environmental alarm.
show fm summary	Displays a summary of FM Information.
show environment status	Displays the information about the operational FRU status.

show cem

To display circuit emulation (CEM) statistics, use the **showcem** command in privileged EXEC mode.

show cem {*slot* / *port* / *channel* | **summary**}

Syntax Description

slot	Slot number where the Circuit Emulation over IP (CEoIP) network module (NM) is installed on the networking device.
/ *port*	Port number on the CEoIP NM. The slash mark is required between the *slot* argument and the *port* argument.
/ *channel*	Channel number that identifies the channel that you want to configure (T1/E1 only). The channel number on a serial port is always 0. The slash mark is required between the *port* argument and the *channel* argument.
summary	Displays summary CEM statistics.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.4(2)T	This command was modified. Output was modified to support enhanced adaptive clocking.

Examples

The following example shows a summary of some of the configuration parameters of the CEM channels.

```
Router# show cem summary
cem summary
cem 1/0/1 is up
Line state is up
Operational state is active
Near end ip address: 192.168.55.130, udp port: 15904
Far end ip address: 192.168.55.136, udp port: 15903
IP payload size: 144
IP dscp : 0x2E Idle pattern length: 8 , Idle Pattern: 0x55
Payload compression is disabled
Data protection is enabled
Dejitter buffer size is 120 ms
Channel clock rate is 512000 bps
CEIP header CRC is disabled
Signaling is enabled, onh:0x0 offh:0xF delay:2000 ms
Failure activation time is 2000 ms
Failure deactivation time is 2000 ms
Physical interface is T1 channelized
Ingress packets: 5044607, dropped: 0, overruns: 0, max_ipt: 3
Egress packets: 5039268, dropped: 0, lost pkts: 52792
Egress late pkts: 222
Egress overruns: 0, underruns: 0, ur_delay: 0, ur2pkt: 0
Egress pkts dropped by burst control: 0
Egress corrupt pkts rcvd: 0
```

```
cem info
30 second ingress rate 513523 bits/sec, 445 packets/sec
30 second egress rate 513100 bits/sec, 445 packets/sec
Tx interrupts: 5035243
Reorder queue flush: 3, visited: 6, max wait window: 4
Pkt-to-pkt jitter max: 141 ms, average: 2 ms, min: 0 ms
Dejitter buffer level max: 118 ms, min: 4 ms
Event history: 0x01830000 Pkts dropped by PCI burst limit: 0
```

The table below describes the significant fields shown in the display.

Table 37: show cem summary Field Descriptions

Field	Description
CEM	Displays the slot, port, and channel number of a CEM channel.
Current State	Displays the current state of a CEM channel. The state can be one of the following: • up--The channel is receiving valid packets from a source CEM channel. • down--The channel is receiving no packets (for example, the dejitter buffer is empty). • shutdown--The CEM channel has been administratively shut down.
Line State	Displays the current line state of a CEM channel. The line state can be one of the following: • up--The line is ready. • down--The line is down. A T1 or E1 line is down when the line is experiencing a physical-layer failure, such as loss of signal (LOS), loss of multiframe alignment (OOF), or alarm indication signal (AIS). A serial line is down when no cable is attached to the port.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Operational State</td><td>Displays the current operational state of a CEM channel. The operational state can be one of the following:
config-incomplete--The channel is in a config-incomplete state when any of the following conditions exist:
An xconnect is not defined.
A local IP address is not defined.
A local UDP port is not defined.
A remote UDP port is not defined.
The CEM channel is administratively shut down.
enabled--If none of the conditions for the config-incomplete state exists, but the CEM channel is receiving no packets from the remote side, the CEM channel is in an enabled state.
config-mismatch--If packets are arriving from the remote side but with a different payload size, data protection setting, or compression setting, the channel is in the config-mismatch state.
active--The CEM channel is active if none of the conditions outlined above exist.</td></tr>
<tr><td>Payload Size</td><td>Payload size configured for the CEM channel, in bytes.</td></tr>
<tr><td>Payload Compression</td><td>Displays whether payload compression is enabled or disabled for the CEM channel.</td></tr>
<tr><td>Data protection</td><td>Displays whether data protection is enabled or disabled for the CEM channel.</td></tr>
<tr><td>MAX_IPT</td><td>Maximum time between two consecutive ingress packets</td></tr>
<tr><td>Egress late packets</td><td>Number of packets that arrive too late to be queued to the dejitter buffer. A packet identified as late packet is discarded and substituted with an idle pattern.</td></tr>
<tr><td>ur_delay</td><td>Delay in milliseconds from the last packet received to the occurrence of an underrun.</td></tr>
<tr><td>ur2pkt</td><td>Delay in milliseconds from the occurrence of an underrun to the reception of the next packet.</td></tr>
<tr><td>pkt-to-pkt-jitter max</td><td>Maximum time between two consecutive egress packets</td></tr>
<tr><td>Dejitter buffer level max</td><td>Maximum recorded level of the dejitter buffer in milliseconds.</td></tr>
</table>

Related Commands

Commands	Description
cem	Enters circuit emulation configuration mode.
clear cem	Clears CEM statistics.

show cem circuit

To display the circuit emulation (CEM) statistics for the configured CEM circuits, use the**showcemcircuit**command in privileged EXEC mode.

show cem circuit [{*cem-group-id* | **interface** {**CEM** | **Virtual-CEM**} *slot*/*subslot*/*port* *cem-group-id* | **detail** | **summary**}]

Syntax Description

cem-group-id	The group ID specified while creating the CEM group.
interface	Displays detailed statistics for a CEM group configured on the specified CEM interface.
CEM	Circuit emulation interface for the data traffic.
Virtual-CEM	Virtual CEM interface created when out-of-band clock recovery is performed on a CEoP SPA.
slot	Slot where SIP-400 is installed.
/ *subslot*	Slot where CEoP SPA is installed. The slash character is required between the*slot* argument and the *subslot* argument.
/ *port*	Port on the CEoP SPA.The slash character is required between the *subslot* argument and the *port* argument.
detail	Displays detailed statistics for all CEM groups.
summary	Displays a summary of CEM groups, as well as their operational modes.

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
15.1(2)SNG	This command was implemented on Cisco ASR 901 Series Aggregation Services Routers.
Cisco IOS XE Everest 16.5.1	This command was implemented on the Cisco ASR 900 Series Routers, Cisco ASR 920 Routers and Cisco NCS 4200 Series.
15.1(2)SNG	This command was implemented on Cisco ASR 901 Series Aggregation Services Routers.

Examples

The following is sample output from the **show cem circuit** command:

```
Router# show cem circuit
CEM Int.       ID   Ctrlr     Admin     Circuit         AC
--------------------------------------------------------------
CEM0/0         0    UP        UP        Enabled         UP
CEM0/1         1    UP        UP        Enabled         UP
CEM0/2         2    UP        UP        Enabled         UP
```

```
CEM0/3         3    UP        UP        Enabled        UP
CEM0/4         4    UP        UP        Enabled        UP
CEM0/5         5    UP        UP        Enabled        UP

Router# show cem circuit 5
CEM0/5, ID: 5, Line: UP, Admin: UP, Ckt: Enabled
Controller state: up
Idle Pattern: 0xFF, Idle cas: 0x8
Dejitter: 4, Sample Rate: 1, Payload Size: 192
Framing: Framed, (DS0 channels: 1-24)
CEM Defects Set
None
Signalling: No CAS
RTP: No RTP
Ingress Pkts:    527521938            Dropped:             0
Egress Pkts:     527521938            Dropped:             0
CEM Counter Details
Input Errors:    0                    Output Errors:       0
Pkts Missing:    0                    Pkts Reordered:      0
Misorder Drops:  0                    JitterBuf Underrun:  0
Error Sec:       0                    Severly Errored Sec: 0
Unavailable Sec: 0                    Failure Counts:      0
Pkts Malformed:  0
```

The following example shows output of the **showcemcircuit**command with the **detail** keyword.

```
Router# show cem circuit detail
CEM2/0/0, ID: 0, Line: UP, Admin: UP, Ckt: ACTIVE
Controller state: up, T1/E1 state: up
Idle Pattern: 0xFF, Idle CAS: 0x8
Dejitter: 5 (In use: 0)
Payload Size: 120
Framing: Framed (DS0 channels: 1-15)
CEM Defects Set
Excessive Pkt Loss Rate Packet Loss
Signalling: No CAS
RTP: No RTP
Ingress Pkts:    715207               Dropped:             0
Egress Pkts:     0                    Dropped:             0
CEM Counter Details
Input Errors:    0                    Output Errors:       0
Pkts Missing:    715234               Pkts Reordered:      0
Misorder Drops:  0                    JitterBuf Underrun:  1
Error Sec:       0                    Severly Errored Sec: 0
Unavailable Sec: 716                  Failure Counts:      1
Pkts Malformed:  0                    JitterBuf Overrun:   0
CEM2/0/0, ID: 1, Line: UP, Admin: UP, Ckt: ACTIVE
Controller state: up, T1/E1 state: up
Idle Pattern: 0xFF, Idle CAS: 0x8
Dejitter: 5 (In use: 0)
Payload Size: 128
Framing: Framed (DS0 channels: 16-31)
CEM Defects Set
Excessive Pkt Loss Rate Packet Loss
Signalling: No CAS
RTP: No RTP
Ingress Pkts:    2306                 Dropped:             0
Egress Pkts:     0                    Dropped:             0
CEM Counter Details
Input Errors:    0                    Output Errors:       0
Pkts Missing:    2306                 Pkts Reordered:      0
Misorder Drops:  0                    JitterBuf Underrun:  1
Error Sec:       0                    Severly Errored Sec: 0
```

```
Unavailable Sec: 0                      Failure Counts:      1
Pkts Malformed:  0                      JitterBuf Overrun:   0
```

The table below describes significant fields shown in the **showcemcircuit** command display.

Table 38: show cem circuit Field Descriptions

Field	Description
CEM	Displays the slot, port, and channel number of a CEM channel.
ID	Displays the value assigned to the CEM group while creating the CEM group.
Controller State	Displays the current state of the controller that represents the CEoP SPA.
Idle Pattern	Specifies the idle pattern that is transmitted on the physical link for any CEM packets that are lost or dropped.
Idle CAS	Specifies the default Channel Associated Signalling (CAS) pattern that is transmitted in the CAS bits of the outgoing T1/E1 frames.
Dejitter	Specifies the size of the dejitter buffer used to compensate for variable network delays experienced by CEM packets.
Payload Size	Specifies the number of payload bytes encapsulated into a single CEM packet.
Framing	Specifies whether the CEM group is framed (CESoPSN) or unframed (SAToP).
CEM Defects Set	Lists the defects that are currently active for the specified CEM group.
CEM Counter Details	Lists the various counters for the CEM group.
Pkts Missing	Specifies the total number of missing packets on the CEM group.
Pkts Reordered	Specifies the number of packets that are arrived out of order on the egress node of the CEM pseudowire and successfully reordered by the CEoP SPA.
Pkts Malformed	Specifies the number of CEM packets that are detected as malformed and dropped.
Misorder Drops	Specifies the number of packets that are dropped because they arrived out of order and could not be reordered.
JitterBuf Underrun	Specifies the number of times the CEoP SPA searches the dejitter buffer for a CEM packet and fails.
JitterBuf Overrun	Specifies the number of times a CEM packet arrived from the pseudowire is not accommodated in the dejitter buffer because the buffer is full.
Error Sec	Specifies the number of seconds in which any missing packet, reorder packet, jitter buffer underrun, misorder dropped packet, or malformed packet is detected.
Severly Errored Sec	Specifies the number of seconds in which more than one percent of the received CEM packets are lost.
Unavailable Sec	Specifies the number of seconds for which the CEM circuit is down due to a fault condition.

Field	Description
Failure Counts	Specifies the number of times the CEM circuit entered into the packet loss state.

show chassis

To display processor and memory information, use the **showchassis** command in privileged EXEC mode.

show chassis [{**clocks** | **slot** *slot-number* [**detail**] | **split** | **detail**}]

Syntax Description

clocks	(Optional) Displays trunk (T1/E1) clock information.
slot *slot-number*	(Optional) Displays slot-specific information.
split	(Optional) Displays split-related data.
detail	(Optional) Displays slot information

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)XB1	This command was introduced on the Cisco AS5850 universal gateway.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **detail** keyword was added. The **clocks** and **split** keywords were removed.

Usage Guidelines

You must enter this command from one of the route-switch-controller (RSC) cards.

Use the **showchassis** command to display additional output relevant to handover-split mode. Command output shows the RSC card to be configured with all slots of the entire chassis, regardless of configured ownership. Slots owned by the peer RSC are shown in the ignore state, properly configured and ready to go.

Examples

The following example shows output for a system in handover-split mode. Each RSC is shown to be configured with all slots in the entire chassis, regardless of whether the RSC actually owns the slot. Slots that are not owned by an RSC are shown to be in the ignore state. The RSC from which the command is entered owns slots 0 to 5, but has configured for it all slots (0 to 5 and 8 to 13--all slots except those in which the RSCs are inserted). Entries for slots 8 and 10 show the designator "ignore."

```
Router# show chassis
System is in handover-split mode, RSC in slot 6.
!
  Slots owned: 0 1 2 3 4 5
  Slots configured: 0 1 2 3 4 5 8 9 10 11 12 13
  Slots owned by other: 8 9 10 11 12 13
Slot    Board        CPU       DRAM                I/O Memory         State     Elapsed
        Type         Util      Total (free)        Total (free)                 Time
5       UP324        0%/0%     26814176( 20%)      33554432( 45%)     Up        01:02:54
8       CT3_UP216    0( 0%)    0( 0%)                                 Ignore    01:05:19
10      UP324        0( 0%)    0( 0%)                                 Ignore    01:05:19
```

The following example shows output for a system in classic-split mode. The RSC from which the command is entered owns slots 0 to 5, and has configured for it only those same slots 0 to 5.

```
Router# show chassis
System is in classic-split mode, RSC in slot 6.
  Slots owned: 0 1 2 3 4 5
  Slots configured: 0 1 2 3 4 5
  Slots owned by other: 8 9 10 11 12 13
```

The following example shows details for the card in slot 0:

```
Router# show chassis slot 0
Slot: 0, Type: 24 E1 Ports (700)
CPU utilization: 0%/0% (5 secs); 0% (1 min); 0% (5 mins)
Memory: Total(b) Used(b) Free(b) Lowest(b) Largest(b)
Processor 59304928 16307688 42997240 42817836 42819352
I/O 67108864 8200288 58908576 58515056 58515004
State: IOS up; elapsed time in state: 13:28:35
Flags:
FB_FLAGS_PRESENT
FB_FLAGS_LINECARD
FB_FLAGS_ANALYZED
FB_FLAGS_CHECKPOINT
Inserted: 13:39:30 ago
Last update: 00:00:08 ago
```

The table below describes significant fields shown in this output.

Table 39: show chassis Fields Descriptions

Field	Description
Slot	Slot number.
Type	Card type.
CPU utilization	CPU usage in percentages.
Memory	Current processor and I/O memory values.
State	Current state of slot and time in hours, minutes, and seconds that the slot has spent in current state.
Flags	Displays a sequence of flag states that the slot has been through.
Inserted	Time in hours, minutes, and seconds since the slot was inserted into the chassis.
Last Update	Time in hours, minutes, and seconds since the last update message was sent.

Related Commands

Command	Description
show dial-shelf	Displays information about dial shelves.

show class cem

T o display the cem parameters configured for CEM class, use the **showclasscem**commandin privilege exec mode. A CEM class helps in configuring parameters in a template and applying parameters at the CEM interface level on a CEOPS SPA.

show class cem [{**name** | **all** | **detail**}]

Syntax Description

name	Indicates the class name, specific to which the CEM parameter details are displayed.
all	Displays the CEM parameter configuration details for all the classes.
detail	Displays CEM parameters configured and additionally provides the circuits and interfaces inheriting the respective class.

Command Default

No default behavior or values.

Command Modes

Privilege Exec Mode (Exec)

Command History

Release	Modification
Cisco IOS XE Release 3.3.0S	This command was introduced.

Usage Guidelines

The **showclasscem**command has been introduced on Cisco ASR 1000 Series Router in Cisco IOS XE Release 3.3. The **showclasscem***name* command is used to view the CEM parameters configured for a specific classname. To view the CEM parameters configured for all the CEM classes, use the **showclasscemall** command. To view the circuits and interfaces inheriting the class and the CEM parameters configured, use the **showclasscemdetail** command from privilege exec mode.

Examples

The following example shows the command output for class parameters configured for a specific class name:

```
Router# show class cem cemqos
Class: DUMMY, Dummy mode: user-defined, Dummy Pattern: 0x77
Class: 0/2/0
Dejitter: 320, Payload Size: 960
```

The following example shows the command output providing details of parameters configured for all the classes and additionally shows the interfaces and circuits inheriting the class:

```
Router# show class cem detail
Class: DUMMY, Dummy mode: user-defined, Dummy Pattern: 0x77
Circuits inheriting this Class:
 None
Interfaces inheriting this Class:
 None
Class: 0/2/0
Dejitter: 320, Payload Size: 960
Circuits inheriting this Class:
 None
```

```
Interfaces inheriting this Class:
 None
```

The following example shows the command output providing details of parameters configured for all the classes:

```
Router# show class cem all

Class: cemqos         , Dummy mode: last-frame
Dejitter: 20, Payload Size: 256
Router#show inter
Router#show interfaces cem 0/1/0
CEM0/1/0 is up, line protocol is up
  Hardware is Circuit Emulation Interface
  MTU 1500 bytes, BW 155520 Kbit/sec, DLY 0 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation CEM, loopback not set
  Keepalive not supported
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 1022000 bits/sec, 745 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     2851672 packets input, 215070144 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
```

Related Commands

Command	Description
clear interface cem	Clears the cem channel.

show compress

To display compression statistics, use the **showcompress** command in user EXEC or privileged EXEC mode.

show compressshow compress command

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
11.3	An example for hardware compression was added as implemented in the Canadian Standards Association (CSA) hardware.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is a sample output from the **showcompress** command when software compression is used on the router:

```
Router# show compress
Serial0
uncompressed bytes xmt/rcv 10710562/11376835
1  min avg ratio xmt/rcv 2.773/2.474
5  min avg ratio xmt/rcv 4.084/3.793
10 min avg ratio xmt/rcv 4.125/3.873
no bufs xmt 0 no bufs rcv 0
resets 0
```

The table below describes the fields shown in the display.

*Table 40: **show compress** Field Descriptions--Software Compression*

Field	Description
Serial0	Name and number of the interface.
uncompressed bytes xmt/rcv	Total number of uncompressed bytes sent and received.
1 min avg ratio xmt/rcv 5 min avg ratio xmt/rcv 10 min avg ratio xmt/rcv	Static compression ratio for bytes sent and received, averaged over 1, 5, and 10 minutes.
no bufs xmt	Number of times buffers were not available to compress data being sent.
no bufs rcv	Number of times buffers were not available to uncompress data being received.

Field	Description
resets	Number of resets (for example, line errors could cause resets).

The following is a sample output from the **showcompress** command when hardware compression is enabled (that is, compression is implemented in the CSA hardware):

```
Router# show compress
 Serial6/1
     Hardware compression enabled
     CSA in slot3 in use
     Compressed bytes sent:     402 bytes     0 Kbits/sec    ratio: 4.092
     Compressed bytes recv:     390 bytes     0 Kbits/sec    ratio: 3.476
     restarts:1
     last clearing of counters: 1278 seconds
```

The table below describes the fields shown in the display. The information displayed by the **showcompress** command is the same for hardware and distributed compression. For Cisco 7200 series routers with multiple CSAs, an additional line is displayed indicating the CSA in use.

Table 41: show compress Field Descriptions--Hardware or Distributed Compression

Field	Description
Serial6/1	Name and number of the interface.
Hardware compression enabled	Type of compression.
CSA in slot3 in use	Identifies the CSA that is performing compression service.
Compressed bytes sent	Total number of compressed bytes sent including the kilobits per second.
Compressed bytes recv	Total number of compressed bytes received including the kilobits per second.
ratio	Compression ratio for bytes sent and received since the link last came up or since the counters were last cleared.
restarts	Number of times the compression process restarted or reset.
last clearing of counters	Duration since the last time the counters were cleared with the **clearcounters**command.

Related Commands

Command	Description
compress	Configures compression for LAPB, PPP, and HDLC encapsulations.

show controllers c3794

To display information about configuration of C37.94 controller, use the **show controllers c3794** command in global configuration mode.

Cisco 900 Series Routers
controllers c3794 *slot/sub-slot/port*

Syntax Description

c3794	Controller type
slot	Backplane slot number. The slot number for C37.94 controller is always 0.
sub-slot	Physical sub-slot number. The range for sub-slot is 0-5.
port	Port number of the controller. Valid numbers are 0 and 3. A forward slash mark (/) is required between the slot argument and the port argument.

Command Modes

Global configuration

Command History

Release	Modification
3.18.1SP	This command was introduced.

Usage Guidelines

This command displays controller status. The information displayed is generally useful for diagnostic tasks performed by technical support personnel only. The command is used to display:

- Number of channels configured
- Number of channels received from tele-protection equipment
- Loss of Signal, if any
- Number of times LOS was set and cleared
- Path of Yellow, if any
- Number of times yellow alarm was set and cleared

Examples

The following is sample output from the **showcontrollers c3794** command on the Cisco 900 Series Router:

```
Router# show controllers c3794
C3794 0/0/0 - (A900-IMA4C3794) is up
Configured Channels: 12
Peer Channels      : 12
Alarm                               : Nil
Sending Y-Alarm to Peer Device      : No
Receiving Y-Alarm from Peer Device : No
```

show controller dsl

To display the DSL controller status and the statistics of a DSL port, use the **showcontrollerdsl** command in privileged EXEC mode.

show controller dsl *slot/port*

Syntax Description

slot	Slot number of the DSL controller.
/ *port*	Port number of the DSL controller. The slash (/) character is required and must be entered when specifying the slot and port arguments.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)XD	This command was introduced on Cisco 2600 series and Cisco 3700 series routers.
12.3(4)XG	This command was integrated into Cisco IOS Release 12.3(4)XG on the Cisco 1700 series routers.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T on Cisco 2600 series, Cisco 3631, and Cisco 3700 series routers.
12.3(11)T	This command was implemented on Cisco 2800 and Cisco 3800 series routers.
12.3(14)T	This command was implemented on Cisco 1800 series routers.

Usage Guidelines

This command is used to display the controller mode of the controller in the specified slot and port and to display the statistics. Use this command in troubleshooting. Use the Cisco IOS help to find the valid slot and port numbers.

Examples

Display for DSL Controller Configured in ATM 4-Wire Mode

The following example displays the status and statistics of the DSL controller in slot 1 and port 0 configured in ATM 4-wire mode:

```
Router# show controller dsl 1/0
 DSL 1/0 controller UP
 Globespan xDSL controller chipset
 DSL mode:SHDSL Annex B
 Frame mode:Utopia
 Configured Line rate:4608Kbps
 Line Re-activated 0 times after system bootup
 LOSW Defect alarm:ACTIVE
 CRC per second alarm:ACTIVE
 Line termination:CO
 FPGA Revision:0xAD
Line 0 statistics
        Current 15 min CRC:0
        Current 15 min LOSW Defect:0
        Current 15 min ES:0
```

```
        Current 15 min SES:0
        Current 15 min UAS:41
        Previous 15 min CRC:0
        Previous 15 min LOSW Defect:0
        Previous 15 min ES:0
        Previous 15 min SES:0
        Previous 15 min UAS:0
Line 1 statistics
        Current 15 min CRC:0
        Current 15 min LOSW Defect:0
        Current 15 min ES:0
        Current 15 min SES:0
        Current 15 min UAS:30
        Previous 15 min CRC:0
        Previous 15 min LOSW Defect:0
        Previous 15 min ES:0
        Previous 15 min SES:0
        Previous 15 min UAS:0
 Line-0 status
 Chipset Version: 1
 Firmware Version: A29733
 Modem Status: Data, Status 1
 Last Fail Mode: No Failure status:0x0
 Line rate: 2312 Kbps
 Framer Sync Status:In Sync
 Rcv Clock Status:In the Range
 Loop Attenuation: 0.600 dB
 Transmit Power: 8.5 dB
 Receiver Gain: 21.420 dB
 SNR Sampling: 39.3690 dB
 Line-1 status
 Chipset Version: 1
 Firmware Version: A29733
 Modem Status: Data, Status 1
 Last Fail Mode: No Failure status:0x0
 Line rate: 2312 Kbps
 Framer Sync Status:In Sync
 Rcv Clock Status:In the Range
 Loop Attenuation: 0.600 dB
 Transmit Power: 8.5 dB
 Receiver Gain: 21.420 dB
 SNR Sampling: 39.1570 dB
 Dying Gasp:Present
```

Display for DSL Controller Configured in T1 Mode

This example shows the display of a DSL controller that has been configured in T1 mode.

```
Router# show controller dsl 0/0
 DSL 0/0 controller UP
 SLOT 0:Globespan xDSL controller chipset
 Line Mode:Two Wire
 DSL mode:SHDSL Annex A
 Frame mode:T1
 Line Re-activated 0 times after system bootup
 LOSW Defect alarm:ACTIVE
 CRC per second alarm:ACTIVE
 Line termination:CPE
 FPGA Revision:0xA9
        Current 15 min CRC:5
        Current 15 min LOSW Defect:0
```

```
        Current 15 min ES:1
        Current 15 min SES:0
        Current 15 min UAS:570
        Previous 15 min CRC:0
        Previous 15 min LOSW Defect:0
        Previous 15 min ES:0
        Previous 15 min SES:0
        Previous 15 min UAS:0
 Line-0 status
 Chipset Version: 1
 Firmware Version: A29733
 Modem Status: Data, Status 1
 Last Fail Mode: No Failure status:0x0
 Line rate: 1552 Kbps
 Framer Sync Status:In Sync
 Rcv Clock Status:In the Range
 Loop Attenuation: 0.7800 dB
 Transmit Power: 7.5 dB
 Receiver Gain: 22.5420 dB
 SNR Sampling: 35.6120 dB
 Dying Gasp:Present
```

Annex Display When Line Is Trained

The following example shows the DSL controller annex display when the line is trained:

```
Router# show controller dsl 1/0
 DSL 1/0 controller UP
 SLOT 0: Globespan xDSL controller chipset
 DSL mode: SHDSL Trained with Annex B-ANFP
```

Annex Display When Line Is Not Trained

The following example shows the DSL controller annex display when the line is not trained:

```
Router# show controller dsl 1/0
 DSL 1/0 controller DOWN
 SLOT 0: Globespan xDSL controller chipset
 DSL mode: Not trained
```

The following table describes the significant fields of the **showcontrollerdsl** command.

Table 42: show controller dsl Field Descriptions

Field	Description
DSL ... controller ...	Describes the status of the controller in the indicated slot number.
DSL mode	Displays the DSL mode of the controller.
Frame mode	Displays the frame mode of the controller.
Configured Line rate	Displays the line rate.
LOSW Defect alarm	Displays the status of the LOSW alarm.

Field	Description
CRC per second alarm	Displays the status of the CRC per second alarm.
Line termination	Displays how the line is terminated.
Chipset Version	Displays the version of the chipset.
Firmware Version	Displays the version of the firmware.
Modem Status	Displays the status of the modem.
Last Fail Mode	Displays the last fail mode.
Line rate	Displays the line rate.
Framer Sync Status	Displays the framer synchronization status.
Rcv Clock Status	Displays the revision clock status.
Loop Attenuation	Displays the loop attenuation.
Transmit Power	Displays the transmit power.
Receiver Gain	Displays the receiver gain.
SNR Sampling	Displays the signal-to-noise ratio sampling.

Related Commands

Command	Description
controller dsl	Configures the controller status and the controller number.

show controller vdsl

To display VDSL controller related information, use the **showcontrollervdsl** command in privileged EXEC mode.

show controller vdsl *slot/subslot/portnumber* [**bit-alloc** | **brief** | **console** | **crash** | **datapath** | **delt-data**| **detailed** | **gain-nsc** | **ipc** | **regs**]

Syntax Description

slot/subslot/port number	Slot, subslot, and port number on the VDSL interface.
bit-alloc	(Optional) Displays bit allocation NSC information.
brief	(Optional) Displays brief information only.
console	(Optional) Displays the console buffer.
crash	(Optional) Displays the CPU crash log.
datapath	(Optional) Displays total datapath information.
delt-data	(Optional) Displays the results of the **delt** command.
detailed	(Optional) Displays all detailed information.
gain-nsc	(Optional) Displays gain NSC information.
ipc	(Optional) Displays ipc statistics.
regs	(Optional) Displays the registers.

Command Default

No default behavior or values

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M1	This command was introduced.

Examples

The following example shows output for this command:

```
router# show controller vdsl 0/0/0
Controller VDSL 0/0/0 is UP
Daemon Status:            Up
                         XTU-R (DS)               XTU-C (US)
Chip Vendor ID:          'BDCM'                    'BDCM'
Chip Vendor Specific:    0x0000                    0x0000
Chip Vendor Country:     0xB500                    0xB500
Modem Vendor ID:         'CSCO'                    'BDCM'
Modem Vendor Specific:   0x4602                    0x0000
Modem Vendor Country:    0xB500                    0xB500
Serial Number Near:     FHH1327000CCISCO00000000
Serial Number Far:
```

```
Modem Version Near:    12.4(20090721:202255) [rahuld-t
Modem Version Far:     0x0000
Modem Status:            TC Sync (Showtime!)
DSL Config Mode:         AUTO
Trained Mode:            G.993.2 (VDSL2)
TC Mode:                 PTM
DELT configuration:      disabled
DELT state:              not running
Trellis:                 ON                       OFF
Line Attenuation:         0.0 dB                  0.0 dB
Signal Attenuation:       0.0 dB                  0.0 dB
Noise Margin:             8.3 dB                  8.2 dB
Attainable Rate:        78548 kbits/s           37743 kbits/s
Actual Power:            10.3 dBm                 8.8 dBm
Per Band Status:        D1      D2      D3      U0      U1      U2      U3
Line Attenuation(dB):   0.1     0.9     N/A     2.2     3.5     8.5     N/A
Signal Attenuation(dB): 0.1     0.9     N/A     N/A     3.1     7.8     N/A
Noise Margin(dB):       8.3     8.2     N/A     N/A     8.2     N/A     N/A
Total FECS:             0                        0
Total ES:               0                        4
Total SES:              0                        4
Total LOSS:             0                        0
Firmware        Source          File Name (version)
--------        ------          -------------------
VDSL            embedded        VDSL_LINUX_DEV_01212008 (1)
Modem FW  Version:      090706_1252-4.02L.01.AvC011b.d21j1
Modem PHY Version:      AvC011b.d21j1
                  DS Channel1     DS Channel0   US Channel1       US Channel0
Speed (kbps):             0            72607            0              37425
Reed-Solomon EC:          0                0            0                  0
CRC Errors:               0                0            0                  0
```

The table below describes the significant fields of the **showcontrollervdsl** command.

Table 43: show controller vdsl Field Descriptions

Field	Description
Daemon Status	Current state of the VDSL daemon, the application that controls the VDSL2 line and the modem state. The VDSL2 daemon can transition through the following states: Reload, Start, Boot Init, Boot Code Download, Firmware Download, DSL Mgmt Task Init, Admin State Check, Configuration, Establishing Link, DSL Line Ready, and Up. The VDSL2 daemon is in the "Up" state when the line reaches showtime.
Chip Vendor ID	Identification code for the chipset vendor, made up of four ASCII characters. For example, BDCM stands for Broadcom.
Chip Vendor Specific	Chipset vendor-specific code made up of four hexadecimal digits as specified in ITU standard. This field is used for ITU standard modes exclusively.
Chip Vendor Country	Country code where the vendor is located. This field is used for ITU standard modes exclusively.
Modem Vendor ID	Identification code for the modem equipment vendor, made up of four ASCII characters. For example, CSCO stands for Cisco.
Modem Vendor Specific	Modem equipment vendor specific code made up of four hexadecimal digits.

Field	Description
Modem Vendor Country	Country code where the modem system vendor is located. This field is used for ITU standard modes exclusively.
Serial Number Near	Serial identification number, which is made up of 11 characters for serial number, 8 characters for platform id, and 11 characters for the version. For example, FOC135145AS 3925-CHA 15.1(2.10)T The 11 characters for the serial number include the modem equipment serial number, modem equipment model, and modem equipment firmware version.
Serial Number Far	Serial identification number of the DSLAM is displayed if it is available from the DSLAM.
Modem Version Near	Modem equipment software version information. It is the IOS version string.
Modem Version Far	Software version of the DSLAM is displayed if it is available from the DSLAM.
Modem Status	Current state of the VDSL2 modem. It can be one of the following states: Line NOT initialized, Line Exception, Idle Request, Silent Request, Line Silent, Handshake, Line FullInit, Discovery, Training, Analysis, Exchange, No Sync, TC Sync (Showtime!), Fast Retrain, Low Power L2, Loop Diagnostics Active, Loop Diagnostics Data Exchange, Loop Diagnostics Data Request, Loop Diagnostics Complete, Resync, Test, Test Loop, Test Reverb, Test Medley, Low Power L3, or Unknown.
DSL Config Mode	VDSL2 line configuration mode. For the HWIC-1VDSL, only Auto mode is supported.
Trained Mode	ITU-T mode in which the VDSL2 line trained up. For the HWIC-1VDSL only G.993.2 (VDSL2) mode is supported.
TC Mode	Layer 2 mode for the VDSL line. For HWIC-1VDSL, only PTM mode is supported.
DELT configuration	Dual Ended Loop Test configuration status, if the feature is enabled.
DELT state	Actual State of Dual Ended Loop Test. The values can be one of the following: Successful, Failed, Not Running, In Progress, or Unknown.
Trellis	Actual State of Dual Ended Loop Test. The values can be one of the following: Successful, Failed, Not Running, In Progress, or Unknown.
Line Attenuation	Aggregate value of Line Attenuation across the subcarriers of all VDSL2 bands.
Signal Attenuation	Aggregate value of Signal Attenuation across the subcarriers of all VDSL2 bands.
Noise Margin	Aggregate value of Signal-to-Noise Ratios (SNR) values across the subcarriers of all VDSL2 bands.
Attainable Rate	Maximum net data rate, in bits, currently attainable by the CPE receiver and DSLAM transmitter.

Field	Description
Actual Power	Measured total output power when the line is trained up. When the line is down, the last measured power is given.
Line Attenuation (dB)	For a band in the downstream direction, it is the measured difference in the total power transmitted by the DSLAM (xTU-C) and the total power received by the CPE (xTU-R) over all sub-carriers of that band during initialization. For a band in the upstream direction, it is the measured difference in the total power transmitted by the xTU-R and the total power received by the xTU-C over all sub-carriers of that band during initialization.
Signal Attenuation (dB)	For a band in the downstream direction, it is the measured difference in the total power transmitted by the DSLAM(xTU-C) and the total power received by the CPE(xTU-R) over all sub-carriers of that band during Showtime. For a band in the upstream direction, it is the measured difference in the total power transmitted by the xTU-R and the total power received by the xTU-C over all sub-carriers of that band during Showtime
Noise Margin (dB)	SNR Margin is the maximum increase of the noise power (in dB) received at the xTU (xTU-R for a band in the downstream direction and xTU-C for a band in the upstream direction), such that the Bit Error Rate (BER) requirements are met for all bearer channels received at the xTU.
Total FECS	Cumulative count during which there is at least one Forward Error Correction (FEC) event on the VDSL2 line.
Total ES	Cumulative count during which there is at least one Errored Second (ES) event on the VDSL2 line.
Total SES	Cumulative count during which there is at least one Severely Errored Second (SES) event on the VDSL2 line.
Total LOSS	Cumulative count, in seconds, during which there is at least one Loss of Signal (LOS) event on the VDSL2 line.
Modem FW Version	Comprehensive firmware version information for the modem, which includes the Operating System version, the VDSL2 PHY version, and the VDSL2 driver version.
Modem PHY Version	Modem firmware Version information, which includes the VDSL2 PHY and the VDSL2 driver.
Speed (kbps)	Actual trained line rate as measured in kbps.
Reed-Solomon EC	Number of VDSL2 superframes that have at least one Reed-Solomon correction action in one of its data frames. Reed-Solomon ECs do not affect service performance.
CRC Errors	Number of superframes that have an incorrect CRC. CRC errors do affect service performance.

Related Commands

Command	Description
clear controller vdsl	Resets the VDSL line related counters.

show controllers analysis-module

To display controller information for the analysis module interface, use the **showcontrollersanalysis-module** command in user EXEC or privileged EXEC mode.

show controllers analysis-module *slot/unit*

Syntax Description

slot	Number of the router chassis slot for the network module.
/ *unit*	Number of the daughter card on the network analysis module (NAM). For NAM, always use 0. The slash (/) between the *slot* and *unit* arguments is required.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.3(4)XD	This command was introduced on the following platforms: Cisco 2600XM series, Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.3(8)T4	This command was implemented on the following platforms: Cisco 2811, Cisco 2821, and Cisco 2851.
12.3(11)T	This command was implemented on the Cisco 3800 series.

Usage Guidelines

The output from this command is generally useful for diagnostic tasks performed by technical support only. Nevertheless, you can use the displayed HARDWARE STATISTICS information to obtain the receive and transmit packet statistics that are collected by the hardware controller during packet processing.

Examples

The following example shows how to display controller information for the analysis module interface when the NAM is installed in router slot 2:

```
Router# show controllers analysis-module 2/0

Interface Analysis-Module2/0
Hardware is Intel 82559 FastEthernet
IDB: 64AD5AB0, FASTSEND: 609A0494, MCI_INDEX: 0
INSTANCE=0x64AD7278
  Rx Ring entries = 64
  Rx Shadow = 0x64AD741C
  Rx Ring = 0x F7C9FE0
  Rx Ring Head = 32
  Rx Ring Last = 31
  Rx Buffer Descr = 0x F7CA420
  Rx Buffer Descr Head = 32
  Rx Buffer Descr Last = 31
  Rx Shadow (malloc) = 0x64AD741C
  Rx Ring (malloc) = 0x4F7C9FE0
  Rx Buffer Descr (malloc) = 0x4F7CA420
  Tx Ring entries = 128
  Tx Shadow = 0x64AD754C
```

```
  Tx Shadow Head = 117
  Tx Shadow Tail = 117
  Tx Shadow Free = 128
  Tx Ring = 0x F7CA860
  Tx Head = 19
  Tx Last = 18
  Tx Tail = 19
  Tx Count = 0
  Tx Buffer Descr = 0x F7CB8A0
  Tx Buffer Descr Head = 0
  Tx Buffer Descr Tail = 0
  Tx Shadow (malloc) = 0x64AD754C
  Tx Ring (malloc) = 0x4F7CA860
  Tx Buffer Descr (malloc) = 0x4F7CB8A0
CONTROL AND STATUS REGISTERS (CSR)=0x3E000000
  SCB Intr Mask    = 00
  SCB CU/RU Cmd    = 00
  SCB Intr Status  = 00
  SCB CU Status    = 01
  SCB RU Status    = 04
  SCB General Ptr  = 00000000
  PORT             = 00000000
  EEPROM           = 0008
  FLASH            = 0002
  MDI              = 1821782D
  Rx Byte Count    = 00000608
  PMDR             = 80
  FC Cmd           = 00
  FC Threshold     = 03
  Early Rx         = 00
  General Status   = 07
  General Control  = 00
PHY REGISTERS
  Register 0x00:   1000  782D  02A8  0154  0501  45E1  0003  0000
  Register 0x08:   0000  0000  0000  0000  0000  0000  0000  0000
  Register 0x10:   0203  0000  0001  0000  0000  0000  0000  0000
  Register 0x18:   0001  0000  8B10  0000  0000  0000  0000  0000
HARDWARE STATISTICS
  Rx good frames:         800
  Rx CRC:                 0
  Rx alignment:           0
  Rx resource:            0
  Rx overrun:             0
  Rx collision detects:   0
  Rx short:               0
  Tx good frames:         614125
  Tx maximum collisions:  0
  Tx late collisions:     0
  Tx underruns:           0
  Tx lost carrier sense:  164
  Tx deferred:            0
  Tx single collisions:   0
  Tx multiple collisions: 0
  Tx total collisions:    0
  FC Tx pause:            0
  FC Rx pause:            0
  FC Rx unsupported:      0
INTERRUPT STATISTICS
  CX  = 613298
  FR  = 805
  CNA = 0
RNR = 0
  MDI = 0
  SWI = 0
```

```
  FCP = 0
Receive All Multicasts = enabled
Receive Promiscuous = disabled
Loopback Mode = disabled
```

The table below describes the significant fields shown in the display.

Table 44: show controllers analysis-module Field Descriptions

Field	Description
Hardware is	Description of the chip being used.
IDB, FASTSEND	Address in router memory of the Interface Descriptor Block (IDB) and the fastsend routine.
INSTANCE	Device-specific data stored in router memory that lists the memory locations and current indexes of receive (Rx) and transmit (Tx) rings in router I/O memory.
CONTROL AND STATUS REGISTERS (CSR)	Control and status registers that are physically located on the chip itself and that are accessed by the CPU over the Peripheral Component Interconnect (PCI) bus.
PHY REGISTERS	Contents of the PHY registers. PHY is a device that interfaces the physical Ethernet line and that is located between the chip and the physical line.
HARDWARE STATISTICS	Receive (Rx) and transmit (Tx) traffic statistics collected by the chip.
INTERRUPT STATISTICS	Transmit (Tx), Receive (Rx), control, software, and flow control interrupt statistics collected by the chip.

Related Commands

Command	Description
service-module analysis-module status	Displays hardware and software status information about the NM-NAM.
show interfaces analysis-module	Displays status, traffic data, and configuration information about the analysis module interface.

show controllers cbus

To display all information under the cBus controller card including the capabilities of the card and reports controller-related failures, use the **showcontrollerscbus** command in privileged EXEC mode on the Cisco 7500 series routers.

show controllers cbus

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(16)	The **showcontrollerscbus** command output display was modified to allow users to monitor IPC buffer limits when **debugcbusipc** is enabled. The **showcontrollerscbus** command output display on the 7500 will now have a new line added under each VIP slot that begins with **ipcacc**. The status line indicates the current ipc accumulator value and its initial limit assigned.

Examples

Cisco 7500 Series Router with VIP2 Card Example

The following is a partial output from the **showcontrollerscbus** command on a Cisco 7500 series router with one Versatile Interface Processor version 2 (VIP2) card. This example does not show output from additional interface processors that are usually installed in a Cisco 7500 series router.

```
Router# show controllers cbus
MEMD at 40000000, 2097152 bytes (unused 2752, recarves 1, lost 0)
  RawQ 48000100, ReturnQ 48000108, EventQ 48000110
  BufhdrQ 48000138 (2849 items), LovltrQ 48000150 (42 items, 1632 bytes)
  IpcbufQ 48000158 (32 items, 4096 bytes)
  3570 buffer headers (48002000 - 4800FF10)
  pool0: 15 buffers, 256 bytes, queue 48000140
  pool1: 368 buffers, 1536 bytes, queue 48000148
  pool2: 260 buffers, 4544 bytes, queue 48000160
  pool3: 4 buffers, 4576 bytes, queue 48000168
slot1: VIP2, hw 2.2, sw 200.50, ccb 5800FF30, cmdq 48000088, vps 8192
    software loaded from system
    FLASH ROM version 255.255
    Fast Ethernet1/0/0, addr 0000.0c41.6c20 (bia 0000.0c41.6c20)
      gfreeq 48000148, lfreeq 480001D0 (1536 bytes), throttled 0
      rxlo 4, rxhi 30, rxcurr 0, maxrxcurr 0
      txq 48001A00, txacc 48001A02 (value 0), txlimit 20
    Ethernet1/1/0, addr 0000.0c41.6c28 (bia 0000.0c41.6c28)
      gfreeq 48000148, lfreeq 480001D8 (1536 bytes), throttled 0
      rxlo 4, rxhi 30, rxcurr 0, maxrxcurr 0
```

```
      txq 48001A08, txacc 48001A0A (value 0), txlimit 20
    Ethernet1/1/1, addr 0000.0c41.6c29 (bia 0000.0c41.6c29)
      gfreeq 48000148, lfreeq 480001E0 (1536 bytes), throttled 0
      rxlo 4, rxhi 30, rxcurr 0, maxrxcurr 0
      txq 48001A10, txacc 48001A12 (value 0), txlimit 20
    Ethernet1/1/2, addr 0000.0c41.6c2a (bia 0000.0c41.6c2a)
      gfreeq 48000148, lfreeq 480001E8 (1536 bytes), throttled 0
      rxlo 4, rxhi 30, rxcurr 0, maxrxcurr 0
      txq 48001A18, txacc 48001A1A (value 0), txlimit 20
    Ethernet1/1/3, addr 0000.0c41.6c2b (bia 0000.0c41.6c2b)
      gfreeq 48000148, lfreeq 480001F0 (1536 bytes), throttled 0
      rxlo 4, rxhi 30, rxcurr 0, maxrxcurr 0
      txq 48001A20, txacc 48001A22 (value 0), txlimit 20
    Ethernet1/1/4, addr 0000.0c41.6c2c (bia 0000.0c41.6c2c)
      gfreeq 48000148, lfreeq 480001F8 (1536 bytes), throttled 0
      rxlo 4, rxhi 30, rxcurr 0, maxrxcurr 0
      txq 48001A28, txacc 48001A2A (value 0), txlimit 20
    Ethernet1/1/5, addr 0000.0c41.6c2d (bia 0000.0c41.6c2d)
      gfreeq 48000148, lfreeq 48000200 (1536 bytes), throttled 0
      rxlo 4, rxhi 30, rxcurr 0, maxrxcurr 0
      txq 48001A30, txacc 48001A32 (value 0), txlimit 20
    Ethernet1/1/6, addr 0000.0c41.6c2e (bia 0000.0c41.6c2e)
      gfreeq 48000148, lfreeq 48000208 (1536 bytes), throttled 0
      rxlo 4, rxhi 30, rxcurr 0, maxrxcurr 0
      txq 48001A38, txacc 48001A3A (value 0), txlimit 20
    Ethernet1/1/7, addr 0000.0c41.6c2f (bia 0000.0c41.6c2f)
      gfreeq 48000148, lfreeq 48000210 (1536 bytes), throttled 0
      rxlo 4, rxhi 30, rxcurr 0, maxrxcurr 0
      txq 48001A40, txacc 48001A42 (value 0), txlimit 20
```

Packet-Over_SONET Interface Processor Example

The following is a partial output from the **showcontrollerscbus** command for a Packet-Over-SONET Interface Processor (POSIP) in slot 0; its single Packet OC-3 interface is Posi0/0.

```
Router# show controllers cbus
slot0: POSIP, hw 2.1, sw 200.01, ccb 5800FF30, cmdq 48000080, vps 8192
    software loaded from flash slot0:rsp_posip.new
    FLASH ROM version 160.4, VPLD version 2.2
    Posi0/0, applique is SONET
      gfreeq 48000148, lfreeq 48000158 (4480 bytes), throttled 0
      rxlo 4, rxhi 226, rxcurr 0, maxrxcurr 186
      txq 48000160, txacc 48000082 (value 150), txlimit 150
```

Multichannel Interface Processor Example

The following is partial output from the **showcontrollerscbus** command for a Multichannel Interface Processor (MIP). Not all of the 23 channels defined on serial interface 1/0 are shown.

```
Router# show controllers cbus
slot1: MIP, hw 1.1, sw 205.03, ccb 5800FF40, cmdq 48000088, vps 8192
    software loaded from system
    T1 1/0, applique is Channelized T1
      gfreeq 48000130, lfreeq 480001B0 (1536 bytes), throttled 0
      rxlo 4, rxhi 360, rxcurr 0, maxrxcurr 3
      Serial1/0:0, txq 480001B8, txacc 48000082 (value 3), txlimit 3
      Serial1/0:1, txq 480001B8, txacc 4800008A (value 3), txlimit 3
      Serial1/0:2, txq 480001B8, txacc 48000092 (value 3), txlimit 3
```

```
Serial1/0:3, txq 480001B8, txacc 4800009A (value 3), txlimit 3
Serial1/0:4, txq 480001B8, txacc 480000A2 (value 3), txlimit 3
Serial1/0:5, txq 480001B8, txacc 480000AA (value 3), txlimit 3
Serial1/0:6, txq 480001B8, txacc 480000B2 (value 3), txlimit 3
Serial1/0:7, txq 480001B8, txacc 480000BA (value 3), txlimit 3
```

The table below describes significant fields in the per-slot part of these displays.

*Table 45: **show controllers cbus** Command--Per-Slot Field Descriptions*

Field	Description
slot1	Slot location of the specific interface processor (in this case Packet-over-SONET Interface Processor).
hw	Version number of the card.
sw	Version number of the card's internal software (in ROM).
software loaded from	Source device and file name from which the router software was loaded.
FLASH ROM version VPLD version	Version of Flash ROM.
Pos1/0, applique is SONET	Location of the specific interface and the hardware applique type (in this case a Packet OC-3 interface).
gfreeq	Location of the global free queue that is shared among similar interfaces.
lfreeq	Location of the local free queue, which is a private queue of MEMD buffers.
throttled	Number of times input packet processing has been throttled on this interface.
rxlo	Minimum number of MEMD buffers held on local free queue. When idle, the interface returns buffers from its local queue to the global free queue until only this number of buffers remain in the local queue.
rxhi	Maximum number of MEMD buffers that the interface can remove from the global free queue in order to populate its local queue.
rxcurr	Number of MEMD buffers currently on the local free queue.
maxrxcurr	Maximum number of MEMD buffers that were enqueued on the local free queue.
txq	Address of the transmit queue.
txacc	Address of the transmit queue accumulator.
txlimit	Maximum number of buffers allowed in the transmit queue.

Cisco 7500 Series Router Example

The following is sample output from the **showcontrollerscbus** command on a Cisco 7500 series router:

```
Router# show controllers cbus
cBus 1, controller type 3.0, microcode version 2.0
  128 Kbytes of main memory, 32 Kbytes cache memory
  40 1520 byte buffers, 14 4484 byte buffers
  Restarts: 0 line down, 0 hung output, 0 controller error
HSCI 1, controller type 10.0, microcode version 129.3
  Interface 6 - Hssi0, electrical interface is Hssi DTE
    5 buffer RX queue threshold, 7 buffer TX queue limit, buffer size 1520
    ift 0004, rql 2, tq 0000 0000, tql 7
    Transmitter delay is 0 microseconds
 MEC 3, controller type 5.1, microcode version 130.6
  Interface 18 - Ethernet2, station address 0000.0c02.a03c (bia 0000.0c02.a03c)
    10 buffer RX queue threshold, 7 buffer TX queue limit, buffer size 1520
    ift 0000, rql 10, tq 0000 0000, tql 7
    Transmitter delay is 0 microseconds
  Interface 19 - Ethernet3, station address 0000.0c02.a03d (bia 0000.0c02.a03d)
    10 buffer RX queue threshold, 7 buffer TX queue limit, buffer size 1520
    ift 0000, rql 10, tq 0000 0000, tql 7
    Transmitter delay is 0 microseconds
```

The table below describes the fields shown in the following lines of output.

```
cBus 1, controller type 3.0, microcode version 2.0
  128 Kbytes of main memory, 32 Kbytes cache memory
  40 1520 byte buffers, 14 4484 byte buffers
  Restarts: 0 line down, 0 hung output, 0 controller error
```

*Table 46: **show controllers cbus** Field Descriptions--Part 1*

Field	Description
cBus 1	Card type and number (varies depending on card).
controller type 3.0	Version number of the card.
microcode version 2.0	Version number of the card's internal software (in ROM).
128 Kbytes of main memory	Amount of main memory on the card.
32 Kbytes cache memory	Amount of cache memory on the card.
40 1520 byte buffers	Number of buffers of this size on the card.
14 4484 byte buffers	Number of buffers of this size on the card.
Restarts • 0 line down • 0 hung output • 0 controller error	Count of restarts for the following conditions: • Communication line down • Output unable to transmit • Internal error

The table below describes the fields shown in the following lines of output:

```
HSCI 1, controller type 10.0, microcode version 129.3
  Interface 6 - Hssi0, electrical interface is Hssi DTE
    5 buffer RX queue threshold, 7 buffer TX queue limit, buffer size 1520
```

```
ift 0004, rql 2, tq 0000 0000, tql 7
Transmitter delay is 0 microseconds
```

*Table 47: **show controllers cbus** Field Descriptions--Part 2*

Field	Description
HSCI 1	Card type and number (varies depending on card).
controller type 10.0	Version number of the card.
microcode version 129.3	Version number of the card's internal software (in ROM).
Interface 6	Physical interface number.
Hssi 0	Logical name for this interface.
electrical interface is Hssi DTE	Self-explanatory.
5 buffer RX queue threshold	Maximum number of buffers allowed in the receive queue.
7 buffer TX queue limit	Maximum number of buffers allowed in the transmit queue.
buffer size 1520	Size of the buffers on this card (in bytes).
ift 0004	Interface type code: • 0 = EIP • 1 = FSIP • 4 = HIP • 5 = TRIP • 6 = FIP • 7 = AIP
rql 2	Receive queue limit. Current number of buffers allowed for the receive queue. It is used to limit the number of buffers used by a particular inbound interface. When equal to 0, all of that interface's receive buffers are in use.
tq 0000 0000	Transmit queue head and tail pointers.
tql 7	Transmit queue limit. Current number of buffers allowed for transmit queue. It limits the maximum cBus buffers allowed to sit on a particular interface's transmit queue.
Transmitter delay is 0 microseconds	Transmitter delay between the packets.

ATM Interface Processor Example

The following is a sample output from the **showcontrollerscbus** command for an ATM Interface Processor (AIP) installed in IP slot 4. The running AIP microcode is Version 170.30, the physical layer interface module (PLIM) type is 4B/5B, and the available bandwidth is 100 Mbps:

```
Router# show controllers cbus
Switch Processor 5, hardware version 11.1, microcode version 170.46
  Microcode loaded from system
  512 Kbytes of main memory, 128 Kbytes cache memory
  60 1520 byte buffers, 91 4496 byte buffers
  Restarts: 0 line down, 0 hung output, 0 controller error
 AIP 4, hardware version 1.0, microcode version 170.30
  Microcode loaded from system
  Interface 32 - ATM4/0, PLIM is 4B5B(100Mbps)
    15 buffer RX queue threshold, 36 buffer TX queue limit, buffer size 4496
    ift 0007, rql 12, tq 0000 0620, tql 36
    Transmitter delay is 0 microseconds
```

Service Provider MultiChannel Interface Processor Example

The following is sample output from the **showcontrollerscbus** command for the Service Provider MultiChannel Interface Processor (SMIP):

```
Router# show controllers cbus
SMIP 2, hardware version 1.0, microcode version 10.0
 Microcode loaded from system
 Interface 16 - T1 2/0, electrical interface is Channelized T1
   10 buffer RX queue threshold, 14 buffer TX queue limit, buffer size 1580 ift 0001, rql
   7, tq 0000 05B0, tql 14
   Transmitter delay is 0 microseconds
```

Per-Slot Limits on IPC Example

The following example shows the current value of the IPC accumulator used for RSP-to-VIP communication along with the initial value of the IPC accumulator assigned to that particular VIP. The IPC accumulator shows the buffers for IPC packets and is analogous to the tx accumulator used for data packets.

```
Router# show controllers cbus
MEMD at E0000000, 2097152 bytes (unused 2880, recarves 1, lost/qaerror recoveries 0/0)
  RawQ E8000100, ReturnQ E8000108, EventQ E8000110, IpcackQ E8000118, VIP_CrashinfoQ E8000128

  IpcSlaveackQ E8000120
  BufhdrQ E8000150 (2893 items), LovltrQ E8000168 (64 items, 2016 bytes)
  IpcbufQ E8000178 (32 items, 4096 bytes)
  IpcbufQ_classic E8000170 (8 items, 4096 bytes)
  3569 buffer headers (E8002000 - E800FF00)
  pool0: 9 buffers, 256 bytes, queue E8000158
  pool1: 298 buffers, 1536 bytes, queue E8000160
  pool2: 261 buffers, 4544 bytes, queue E8000180
  pool3: 4 buffers, 4576 bytes, queue E8000188
  slot1: VIP2 R5K, hw 2.00, sw 22.20, ccb F800FF20, cmdq E8000088, vps 8192
    software loaded from system
    Copyright (c) 1986-2005 by Cisco Systems, Inc.
```

```
    ROM Monitor version 115.0
    ipcacc E8000082 (value 17), ipclimit 36
    FastEthernet1/0/0, addr 0050.0b35.5820 (bia 0050.0b35.5820)
      gfreeq E8000160, lfreeq E8000190 (1536 bytes)
      rxlo 4, rxhi 123, rxcurr 0, maxrxcurr 0
      txq E8001A00, txacc E8001A02 (value 0), txlimit 33
    ATM1/1/0, applique is OC3 (155000Kbps)
      gfreeq E8000180, lfreeq E8000198 (4544 bytes)
      rxlo 4, rxhi 261, rxcurr 0, maxrxcurr 0
      txq E8001A08, txacc E8001A0A (value 0), txlimit 174
  slot2: VIP4-50 RM5271, hw 2.01, sw 22.20, ccb F800FF30, cmdq E8000090, vps 8192
    software loaded from system
    Copyright (c) 1986-2005 by Cisco Systems, Inc.
    ROM Monitor version 103.0
    ipcacc E800008A (value 36), ipclimit 36
    ATM2/0/0, applique is SONET (155000Kbps)
```

show controllers cbus Display With a Filter Applied to Customize the Display

The following example shows the IPC statistics. The **showcontrollerscbus** command output display on the 7500 includes a line under the entry for each VIP slot that begins with **ipcacc**. The status line indicates the current IPC accumulator value and its initial limit assigned.

```
Router# show controllers cbus | include ipc|slot
  slot1: VIP2 R5K, hw 2.00, sw 22.20, ccb F800FF20, cmdq E8000088, vps 8192
    ipcacc E8000082 (value 6), ipclimit 36
  slot2: VIP4-50 RM5271, hw 2.01, sw 22.20, ccb F800FF30, cmdq E8000090, vps 8192
    ipcacc E800008A (value 36), ipclimit 36
  slot3: VIP2 R5K, hw 2.00, sw 22.20, ccb F800FF40, cmdq E8000098, vps 8192
    ipcacc E8000092 (value 6), ipclimit 36
```

When the IPC acc reaches 10% of the IpcbufQ limit, a rate-limited warning message will be displayed if the **debugcbusipc** comamnd is enabled:

```
%RSP-6-IPC_STUCK: Ipcacc for slot 1 has reached 7% of its Ipclimit
```

show controllers content-engine

To display controller information for content engine (CE) network modules, use the **showcontrollerscontent-engine** command in privileged EXEC mode.

show controllers content-engine *slot*/*unit*

Syntax Description

slot	Number of the router chassis slot for the network module.
/ *unit*	Number of the daughter card on the network module. For CE network modules, always use 0. The slash (/) character is required when specifying the *slot* and *unit* arguments.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)YT	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Examples

The following example displays controller information for the CE network module in router slot 1:

```
Router# show controllers content-engine 1/0
Interface Content-Engine1/0
Hardware is Intel 82559 FastEthernet
IDB: 82A92DC4, FASTSEND: 8021B488, MCI_INDEX: 0
INSTANCE=0x82A94534
  Rx Ring entries = 64
  Rx Shadow = 0x82A947A0
  Rx Ring = 0x 3CB5160
  Rx Ring Head = 14
  Rx Ring Last = 13
  Rx Buffer Descr = 0x 3CB55A0
  Rx Buffer Descr Head = 14
  Rx Buffer Descr Last = 13
  Rx Shadow (malloc) = 0x82A947A0
  Rx Ring (malloc) = 0x 3CB5160
  Rx Buffer Descr (malloc) = 0x 3CB55A0
  Tx Ring entries = 128
  Tx Shadow = 0x82A948D0
  Tx Shadow Head = 79
  Tx Shadow Tail = 79
  Tx Shadow Free = 128
  Tx Ring = 0x 3CB59E0
  Tx Head = 81
  Tx Last = 80
  Tx Tail = 81
  Tx Count = 0
  Tx Buffer Descr = 0x 3CB6A20
  Tx Buffer Descr Head = 0
  Tx Buffer Descr Tail = 0
  Tx Shadow (malloc) = 0x82A948D0
  Tx Ring (malloc) = 0x 3CB59E0
  Tx Buffer Descr (malloc) = 0x 3CB6A20
```

```
CONTROL AND STATUS REGISTERS (CSR)=0x40800000
  SCB Intr  Mask   = 00
  SCB CU/RU Cmd    = 00
  SCB Intr  Status = 00
  SCB CU/RU Status = 50
  SCB General Ptr  = 00000000
  PORT             = 00000000
  EEPROM           = 0008
  FLASH            = 0002
  MDI              = 1821782D
  Rx Byte Count    = 00000608
  PMDR             = 80
  FC Cmd           = 00
  FC Threshold     = 03
  Early Rx         = 00
  General Status   = 05
  General Control  = 00
PHY REGISTERS
  Register 0x00:   1000  782D  02A8  0154  0441  45E1  0001  0000
  Register 0x08:   0000  0000  0000  0000  0000  0000  0000  0000
  Register 0x10:   0401  0000  0001  0000  0000  0000  0000  0000
  Register 0x18:   0000  0000  8000  0000  0000  0000  0000  0000
HARDWARE STATISTICS
  Rx good frames:         14
  Rx CRC:                 0
  Rx alignment:           0
  Rx resource:            0
  Rx overrun:             0
  Rx collision detects:   0
  Rx short:               0
  Tx good frames:         79
  Tx maximum collisions:  0
  Tx late collisions:     0
  Tx underruns:           0
  Tx lost carrier sense:  0
  Tx deferred:            0
  Tx single collisions:   0
  Tx multiple collisions: 0
  Tx total collisions:    0
  FC Tx pause:            0
  FC Rx pause:            0
  FC Rx unsupported:      0
INTERRUPT STATISTICS
  CX  = 613298
  FR  = 805
  CNA = 0
RNR = 0
  MDI = 0
  SWI = 0
  FCP = 0
  Receive All Multicasts = enabled
  Receive Promiscuous = disabled
  Loopback Mode = disabled
```

The table below describes the significant fields shown in the display.

Table 48: show controllers content-engine Field Descriptions

Field	Description
Hardware	Description of the chip being used.

Field	Description
IDB, FASTSEND	Address in router memory of the Interface Descriptor Block (IDB) and the fastsend routine.
INSTANCE	Device-specific data stored in router memory that lists the memory locations and current indices of receive (Rx) and transmit (Tx) rings in router I/O memory.
CONTROL AND STATUS REGISTERS (CSR)	Control and status registers that are physically located on the chip itself and that are accessed by the CPU over the protocol control information (PCI) bus.
PHY REGISTERS	Contents of the physical layer (PHY) registers. A PHY module is a device that interfaces the physical Ethernet line and that is located between the chip and the physical line.
HARDWARE STATISTICS	Receive (Rx) and transmit (Tx) traffic statistics collected by the chip.
INTERRUPT STATISTICS	Transmit (Tx), Receive (Rx), control, software, and flow control interrupt statistics collected by the chip.

Related Commands

Command	Description
interface content-engine	Configures an interface for a CE network module and enters interface configuration mode.
show interfaces content-engine	Displays basic interface configuration information for a CE network module.

show controllers dsx3

To display digital signal level 3 cross connect (dsx3) information and to display hardware and software driver information for the dsx3 controller, use the **showcontrollersdsx3**command in privileged EXEC mode.

show controllers dsx3 *shelf* / *slot* / *port*

Syntax Description

shelf	Shelf chassis in the Cisco 10000 series router that contains the dsx3 interface card.
/*slot*	Location of the dsx3 interface card in the shelf chassis.
/*port*	Port number.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(31)SB	This command was introduced in a release earlier to Cisco IOS Release 12.2(31)SB.
12.2(33)SB	This command's behavior was modified on the Cisco 10000 series router for the PRE3 and PRE4.

Examples

The following is a sample output show the show controller dsx3 command for 8E3DS3 card:

```
Router# show controllers dsX3 3/0/0
DSX3 3/0/0 is down.  Hardware is C10K ET line card
  ET H/W Version : 0.0.0, ET ROM Version : 0.0, ET F/W Version : 0.0.0
  Applique type is Subrate T3/E3
  Receiver has loss of signal.
  MDL transmission is disabled

  FEAC code received: No code is being received
  Framing is C-BIT Parity (Configured)
  Line Code is B3ZS, Clock Source is Internal
  DSU mode is cisco, DSU bandwidth is 44210
  equipment customer loopback
  Data in current interval (75 seconds elapsed):
     0 Line Code Violations, 0 P-bit Coding Violation
     0 C-bit Coding Violation, 0 P-bit Err Secs
     0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
     75 Unavailable Secs, 0 Line Errored Secs
     0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
     0 AIS Defect Secs, 75 LOS Defect Secs
     0 Near-end path failures
     0 Far-end path failures, 0 FERF Defect Secs
     0 CP-bit Far-End Unavailable Secs, 0 Far-End Coding Violations
     0 Far-End Errored Secs, 0 Far-End Severely Errored Secs
```

The table below describes the significant fields shown in the display.

Table 49: show controllers dsx3 Field Descriptions--Cisco 10000 series router

Field	Description
AIS	The alarm indication signal (AIS).
dsx3 3/0/0 is down	dsx3 controller connected to this Cisco 10000 series router in shelf 3, slot 0, port 0 is down. The controller's state can be up, down, or administratively down. Loopback conditions are shown by Locally Looped or Remotely Looped.
Applique type	Describes the type of controller.
No alarms detected	Any alarms detected by the controller are displayed here. Possible alarms are as follows: • Receiver has loss of frame (LOF). • Receiver has loss of signal (LOS). • Receiver has no alarms. • Receiver has remote alarm. • Receiver is getting AIS. • Transmitter is sending alarm indication signal (AIS). • Transmitter is sending remote alarm.
MDL transmission	Maintenance Data Link status (either enabled or disabled). Used for carrying performance information and control signals across the network toward the far-end dsx3 unit.
FEAC code received	Whether a far-end alarm code request is being received. Possible values are as follows: • Common Eqpt. Failure (NSA) • DS1 Eqpt. Failure (NSA) • DS1 Eqpt. Failure • DS3 AIS Received • DS3 Eqpt. Failure (NSA) • DS3 Eqpt. Failure (SA) • DS3 IDLE Received • DS3 LOS/HBER • DS3 Out-of-Frame • Multiple DS1 LOS/HBER • No code is being received • Single DS1 LOS/HBER

Field	Description
Framing	Standard dsx3 framing type: M23, C-bit, or Auto-detect.
Line Code	Standard dsx3 line-coding format. In the example, the line-coding format is bipolar 3-zero substitution (B3ZS).
Clock Source	The source of the synchronization signal (clock): Line or Internal. In this example, the line is providing the clock signal.
Data in current interval (seconds elapsed)	Summary statistics for dsx3 signal quality for the current time interval of 900 seconds (15 minutes). In this example, the statistics are for current partial interval. Statistics roll into the 24-hour accumulation buffer every 15 minutes. The oldest 15-minute period falls off the back of the 24-hour accumulation buffer.
Line Code Violations	Count of both Bipolar Violations (BPVs) and Excessive Zeros (EXZs) that occur over the accumulation period. An EXZ increments the line code violations (LCVs) by one, regardless of the length of the zero string.
P-bit Coding Violation	P-bit parity error event. A P-bit parity error event is the occurrence of a received P-bit code on the DS3 M-frame that is not identical to the corresponding locally calculated code. Referred to as PCV.
C-bit Coding Violation	Count of coding violations reported via the C-bits. For C-bit parity, it is the count of CP-bit parity errors that occur during the accumulation interval. Referred to as CCV.
P-bit Err Secs	Number of seconds with one or more PCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when unavailable seconds are counted.
P-bit Severely Err Secs	Number of seconds with 44 or more PCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when unavailable seconds are counted.
Severely Err Framing Secs	Number of a seconds with one or more out-of-frame defects or a detected incoming AIS.
Unavailable Secs	Number of seconds during which the interface was not available in this interval. Referred to as UAS.
Line Errored Secs	Number of seconds in this interval during which one or more code violations or one or more LOS defects occurred. Referred to as LES.
C-bit Errored Secs	Number of seconds with one or more C-bit code violations (CCV), one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when UASs are counted. Referred to as CES.
C-bit Severely Errored Secs	Number of seconds with 44 or more CCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when UASs are counted.

show controller dwdm

To display ITU-T G.709 alarms, alerts, and counters for a dense wavelength division multiplexing (DWDM) controller, use the **showcontrollerdwdm**command in privileged EXEC mode.

show controller dwdm *slot/port* [**g709**]

Syntax Description

slot	Chassis slot number of the DWDM controller.
/ *port*	Port number of the DWDM controller.
g709	(Optional) Displays G.709 information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRD1	This command was introduced on the Cisco 7600 series routers.

Examples

The following is sample output from the **showcontrollerdwdm**command. The output fields are self-explanatory.

```
Router# show controller dwdm 2/3

 Controller dwdm 2/3, is up (operational state)
G709 status : Enabled

OTU
        LOS = 5             LOF = 5             LOM = 0
        AIS = 0             BDI = 1             BIP = 0
        TIM = 0             IAE = 4             BEI = 0

ODU
        AIS = 0             BDI = 0             TIM = 0
        OCI = 0             LCK = 0             PTIM = 5
        BIP = 0             BEI = 0

FEC Mode: FEC
        EC(current second) = 13539920
        EC = 1750575661   UC = 1356085

        pre-FEC BER = 121981.2578E-8

         Q = 2.9677             Q Margin =  0.5052 dBQ

Detected Alarms: NONE
Asserted Alarms: NONE
Detected Alerts: NONE
Asserted Alerts: NONE
Alarm reporting enabled for: LOS LOF LOM OTU-AIS OTU-IAE OTU-BDI OTU-TIM ODU-AIS ODU-OCI
ODU-LCK ODU-BDI ODU-PTIM ODU-TIM
Alert reporting enabled for: OTU-SM-TCA ODU-SD-BER ODU-SF-BER ODU-PM-TCA
```

```
BER thresholds: ODU-SF = 10e-3  ODU-SD = 10e-6
TCA thresholds: SM = 10e-3  PM = 10e-3
```

Related Commands

Command	Description
show platform dwdm alarm history	Displays platform DWDM alarm history.

show controllers e1

To display information about E1 links, use the **showcontrollerse1**command in privileged EXEC mode.

Cisco 4000 Series Routers
show controllers e1 *controller-number*

Cisco 7500 Series Routers and Cisco ASR 901 Series Routers
show controllers e1 [*slot/port*]

Cisco AS5000 Series Access Servers
show controllers e1 {*controller-number* | **clock** | **firmware-status** | **monitor** | **timeslots** *timeslot-range*}

Cisco Series
show controllers e1 [*slot/bay/port*]

Syntax Description

controller-number	Controller number.
slot / *port*	(Optional) Backplane slot number and port number on the interface. Refer to the hardware manuals for your controller type to determine specific slot and port numbers.
slot / *bay* / *port*	Slot number, interface module number in which the slot is inserted, and port number (Cisco series routers).
clock	Displays primary clock change history.
firmware-status	Displays system crash history.
monitor	Displays primary monitor change history.
timeslots *timeslot-range*	Displays DS0 information. Time slot range is 1 through 31 for the E1 controller.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
11.2	This command was implemented on additional router platforms.
12.1(3)T	This command was implemented on additional access server platforms.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.4(3)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Release	Modification
XE Everest 16.5.1	This command was implemented on the Cisco ASR 900 Series Routers and Cisco NCS 4200 Series.
XE Fuji 16.8.x	This command output was modified on the Cisco Series Routers to display far-end counters for performance monitoring.

Usage Guidelines

This command displays controller status that is specific to the controller hardware. The information displayed is generally useful for diagnostic tasks performed by technical support personnel only.

The Network Processor Module (NPM) on the Cisco 4000 series router or MultiChannel Interface Processor (MIP) on a Cisco 7500 series router can query the port adapters to determine their current status. Issue a **showcontrollerse1** command to display statistics about the E1 link.

On a Cisco 7500 series router, if you specify a slot and port number each 15-minute period will be displayed.

On the Cisco 5000 series access servers use the **showcontrollerse1timeslots** command to display the CAS and ISDN PRI channel state in detail. This command shows whether the DS0 channels of a controller are in idle, in-service, maintenance, or busyout states. Enter the commands to display statistics about the E1 links.

Examples

The following is sample output from the **showcontrollerse1** command on the Cisco 7500 series router:

```
Router# show controllers e1
e1 0/0 is up.
  Applique type is Channelized E1 - unbalanced
  Framing is CRC4, Line Code is HDB3
  No alarms detected.
  Data in current interval (725 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
  Total Data (last 24 hours)
     0 Line Code Violations, 0 Path Code Violations,
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins,
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
```

The following is sample output from the **showcontrollerse1**command including the board identifier type:

```
Router#
show controllers e1
E1 4/1 is up.
  No alarms detected.
  Framing is CRC4, Line Code is hdb3
  Data in current interval (0 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations 0 Slip Secs, 0 Fr Loss Secs,
     0 Line Err Secs, 0 Degraded Mins 0 Errored Secs, 0 Bursty Err Secs,
     0 Severely Err Secs, 0 Unavail Secs
  Total Data (last 79 15 minute intervals):
     0 Line Code Violations, 0 Path Code Violations, 0 Slip Secs, 0 Fr Loss Secs,
     0 Line Err Secs, 0 Degraded Mins, 0 Errored Secs, 0 Bursty Err Secs,
     0 Severely Err Secs, 0 Unavail Secs
```

The table below describes the significant fields shown in the display.

Table 50: show controllers e1 Field Descriptions

Field	Description
e1 0/0 is up	The E1 controller 0 in slot 0 is operating. The controller's state can be up, down, or administratively down. Loopback conditions are shown by (Locally Looped) or (Remotely Looped).
Applique type	The applique type is shown and will indicate balanced or unbalanced.
Framing is	Displays the current framing type.
Linecode is	Displays the current linecode type.
No alarms detected	Any alarms detected by the controller are displayed here. Possible alarms are as follows: • Transmitter is sending remote alarm. • Transmitter is sending AIS. • Receiver has loss of signal. • Receiver is getting AIS. • Receiver has loss of frame. • Receiver has remote alarm. • Receiver has no alarms.
Data in current interval (725 seconds elapsed)	Displays the current accumulation period, which rolls into the 24-hour accumulation every 15 minutes. Accumulation period is from 1 to 900 seconds. The oldest 15-minute period falls off the back of the 24-hour accumulation buffer.
Line Code Violations	Indicates the occurrence of either a Bipolar Violation (BPV) or Excessive Zeros (EXZ) error event.
Path Code Violations	Indicates a frame synchronization bit error in the D4 and E1-no-CRC formats, or a cyclic redundancy check (CRC) error in the Extended Superframe (ESF) and E1-CRC formats.
Slip Secs	Indicates the replication or deletion of the payload bits of a DS1 frame. A slip might be performed when there is a difference between the timing of a synchronous receiving terminal and the received signal.
Fr Loss Secs	Indicates the number of seconds an Out Of Frame (OOF) error is detected.
Line Err Secs	Line Errored Seconds (LES) is a second in which one or more Line Code Violation errors are detected.
Degraded Mins	A Degraded Minute is one in which the estimated error rate exceeds 1E-6 but does not exceed 1E-3.

Field	Description
Errored Secs	In ESF and E1 CRC links, an Errored Second is a second in which one of the following are detected: one or more Path Code Violations; one or more Out of Frame defects; one or more Controlled Slip events; a detected AIS defect. For SF and E1 no-CRC links, the presence of Bipolar Violations also triggers an Errored Second.
Bursty Err Secs	A second with fewer than 320 and more than 1 Path Coding Violation error, no Severely Errored Frame defects and no detected incoming AIS defects. Controlled slips are not included in this parameter.
Severely Err Secs	For ESF signals, a second with one of the following errors: 320 or more Path Code Violation errors; one or more Out of Frame defects; a detected AIS defect. For E1-CRC signals, a second with one of the following errors: 832 or more Path Code Violation errors; one or more Out of Frame defects. For E1-nonCRC signals, a second with 2048 Line Code Violations or more. For D4 signals, a count of 1-second intervals with Framing Errors, or an Out of Frame defect, or 1544 Line Code Violations.
Unavail Secs	A count of the total number of seconds on the interface.

The following is sample output from the **showcontrollerse1timeslots** command on a Cisco access server. The information displayed is self-explanatory.

```
Router# show controllers e1 timeslots 1
SERVICE STATES               CAS CHANNEL STATES
insvc     = In Service         down        = Down
outofsvc = Out of Service     idle        = Idle
maint    = Maintenance        connected  = Call Connected
                              signaling  = Signaling
                              static-bo  = Static Busyout
                              dynamic-bo = Dynamic Busyout
                              ISDN CHANNEL STATES
                              idle       = Available
                              proposed   = Negotiating
                              busy       = Unavailable
                              reserved   = Reserved
                              restart    = Restart Pending
                              maint_pend = Maintenance Pending
                              reassigned = Reassigned
                              prop'd_1tr6= Net may change channel #
```

Series Router

The following is sample output from the **show controllers e1** command on the Cisco series routers:

```
Router# show controllers e1 0/2/1
E1 0/2/1 is up.
Hardware is -48T3E3-CE
No alarms detected.
MDL transmission is disabled
FEAC code received: No code is being received
```

```
Framing is C-BIT Parity, Line Code is B3ZS, Cablelength Short less than 225ft
BER thresholds: SF = 10e-10 SD = 10e-10
Clock Source is internal
Equipment customer loopback
Data in current interval (240 seconds elapsed):
Near End
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavailable Secs
     0 Path Failures, 0 SEF/AIS Secs
   Far End
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavailable Secs
     0 Path Failures
  Data in Interval 1:
   Near End
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 14 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 15 Unavailable Secs
     1 Path Failures, 0 SEF/AIS Secs
   Far End Data
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 4 Fr Loss Secs, 2 Line Err Secs, 0 Degraded Mins
     4 Errored Secs, 0 Bursty Err Secs, 4 Severely Err Secs, 0 Unavailable Secs
     0 Path Failures
  Total Data (last 1 15 minute intervals):
   Near End
     0 Line Code Violations, 0 Path Code Violations,
     0 Slip Secs, 0 Fr Loss Secs, 14 Line Err Secs, 0 Degraded Mins,
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 15 Unavailable Secs
     1 Path Failures, 0 SEF/AIS Secs
   Far End
     0 Line Code Violations, 0 Path Code Violations,
     0 Slip Secs, 4 Fr Loss Secs, 2 Line Err Secs, 0 Degraded Mins,
     4 Errored Secs, 0 Bursty Err Secs, 4 Severely Err Secs, 0 Unavailable Secs
     0 Path Failures
```

Examples

show controllers e3

To display information about an E3 controller, use the**showcontrollerse3**command in user EXEC or privileged EXEC mode.

show controllers e3 *slot/port* [{**brief** | **tabular**}]

Series
show controllers e3 [*slot/bay/port*]

Syntax Description

slot	Slot number. Refer to the appropriate hardware manual for slot information.
/ *port*	Port number. Refer to the appropriate hardware manual for port information.
brief	(Optional) Displays a list of configurations only.
tabular	(Optional) Displays a list of configurations and MIB information in a tabular format.
slot / bay / port	Slot number, interface module number in which the slot is inserted, and port number (Cisco series routers).

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
11.1 CC	This command was introduced on the E3 controller.
12.2(11)YT	This command was integrated into Cisco IOS Release 12.2(11)YT and implemented on the following platforms: Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3660 series, Cisco 3725, and Cisco 3745 routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
XE Fuji 16.8.x	This command output was modified on the Cisco ASR 900 Series and Cisco NCS 4200 Series Routers to display far-end counters for performance monitoring.

Examples

The following are samples of output from the **showcontrollerse3**command:

```
Router# show controllers e3 2/0
E3 2/0 is down.
 Applique type is Subrate E3
 Transmitter is sending remote alarm.
 Receiver has loss of signal.
 Framing is G751, Clock Source is Internal.
 Data in current interval (450 seconds elapsed):
  0 C-bit Coding Violation
  0 P-bit Err Secs, 0 P-bit Severely Err Secs
  0 Severely Err Framing Secs, 450 Unavailable Secs
  0 Line Errored Secs, 0-C-bit Errored Secs, 0 C-bit Severely Errored Secs
 Data in Interval 1:
  0 C-bit Coding Violation
  0 P-bit Err Secs, 0 P-bit Severely Err Secs
```

```
  0 Severely Err Framing Secs, 900 Unavailable Secs
  0 Line Errored Secs, 0-C-bit Errored Secs, 0 C-bit Severely Errored Secs
 Total Data (last 1 15 minute intervals):
  0 C-bit Coding Violation
  0 P-bit Err Secs, 0 P-bit Severely Err Secs
  0 Severely Err Framing Secs, 900 Unavailable Secs
0 Line Errored Secs, 0-C-bit Errored Secs, 0 C-bit Severely Errored Secs
Router# show controllers e3 2/0 brief
E3 2/0 is down.
  Applique type is Subrate E3
  Transmitter is sending remote alarm.
  Receiver has loss of signal.
  Framing is G571, Clock Source is Internal.
Router# show controllers e3 2/0 tabular
E3 2/0 is down.
  Applique type is Subrate E3
  Transmitter is sending remote alarm.
  Receiver has loss of signal.
  Framing is G571, Clock Source is Internal.
  INTERNAL   LCV PCV CCV PES PSES SEFS UAS LES CES CSES
  18:10-18:21 0   0   0   0   0    0   680  0   0    0
  17:55-18:10 0   0   0   0   0    0   900  0   0    0
  Total       0   0   0   0   0    0   900  0   0    0
```

The table below describes the significant fields shown in the display.

Table 51: show controllers e3 Field Descriptions

Field	Description
E3 2/0 is down	The E3 controller in slot 0 shows the state in which it is operating. The controller's state can be up, down, or administratively down. Loopback conditions are shown by (Locally Looped) or (Remotely Looped).
Applique type	Controller type.
Description	User-specified information about the E3 controller.
No alarms detected (not shown in display)	Any alarms detected by the controller are displayed here. Possible alarms are as follows: • Transmitter is sending remote alarm. • Transmitter is sending alarm indication signal (AIS). • Receiver has loss of signal. • Receiver is getting AIS. • Receiver has loss of frame. • Receiver has remote alarm. • Receiver has no alarms.
Linecode is (not shown in display)	Line coding format on the E3.
Framing	Framing type.

Field	Description
Clock Source	User-specified clock source (Line or Internal).
Data in current interval (450 seconds elapsed)	Shows the current accumulation period, which rolls into the 24-hour accumulation every 15 minutes. Accumulation period is from 1 to 900 seconds. The oldest 15-minute period falls off the back of the 24-hour accumulation buffer.
PCV	Path coding violation (PCV) error event is a frame synchronization bit error in the E1-no-CRC formats or a cyclic redundancy check (CRC) error in the E1-CRC formats.
CCV	C-bit coding violation (CCV) error event for C-bit parity. This is the count of coding violations reported via the C-bits occurring in the accumulation interval.
PES	P-bit errored seconds (PES) is a second with one or more PCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when unavailable seconds are counted.
PSES	P-bit severely errored seconds (PSES) is a second with 44 or more PCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when unavailable seconds are counted.
SEFS	Severely errored framing seconds (SEFS) is a second with one or more out-of-frame defects or a detected incoming AIS.
UAS	Unavailable seconds (UAS) are calculated by counting the number of seconds for which the interface is unavailable. For more information, refer to RFC 1407.
LES	Line errored seconds (LES) is a second in which one or more code violations or one or more LOS defects occurred.
CES	C-bit errored seconds (CES) is a second with one or more out-of-frame defects or a detected incoming AIS. This gauge is not incremented when UASs are counted.
CSES	C-bit severely errored seconds (CSES) is a second with one or more out-of-frame defects or a detected incoming AIS. This gauge is not incremented when UASs are counted.
Total	Displays the last 15-minute accumulation period.

Series Router

The following is sample output from the **show controllers e3** command on the Cisco series routers:

```
Router# show controllers e3 0/4/40
E3 0/4/40 is up.
Hardware is -48T3E3-CE
Applique type is Clear Channel e3
No alarms detected.
MDL transmission is disabled
FEAC code received: No code is being received
```

```
Framing is C-BIT Parity, Line Code is B3ZS, Cablelength Short less than 225ft
BER thresholds: SF = 10e-10 SD = 10e-10
Clock Source is internal
Equipment customer loopback
Data in current interval (240 seconds elapsed):
 Near End
     0 Line Code Violations, 0 P-bit Coding Violations
     0 C-bit Coding Violations, 0 P-bit Err Secs
     0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
     0 Unavailable Secs, 0 Line Errored Secs
     0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
     0 Severely Errored Line Secs, 0 Path Failures
     0 AIS Defect Secs, 0 LOS Defect Secs
   Far End
     0 Errored Secs, 0 Severely Errored Secs
     0 C-bit Unavailable Secs, 0 Path Failures
     0 Code Violations, 0 Service Affecting Secs
  Data in Interval 1:
   Near End
     0 Line Code Violations, 0 P-bit Coding Violations
     0 C-bit Coding Violations, 0 P-bit Err Secs
     0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
     20 Unavailable Secs, 20 Line Errored Secs
     0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
     20 Severely Errored Line Secs, 1 Path Failures
     0 AIS Defect Secs, 20 LOS Defect Secs
   Far End
     0 Errored Secs, 0 Severely Errored Secs
     0 C-bit Unavailable Secs, 0 Path Failures
     0 Code Violations, 0 Service Affecting Secs
  Total Data (last 1 15 minute intervals):
   Near End
     0 Line Code Violations, 0 P-bit Coding Violations,
     0 C-bit Coding Violations, 0 P-bit Err Secs,
     0 P-bit Severely Err Secs, 0 Severely Err Framing Secs,
     20 Unavailable Secs, 20 Line Errored Secs,
     0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
     20 Severely Errored Line Secs, 1 path failures
     0 AIS Defect Secs, 20 LOS Defect Secs
   Far End
     0 Errored Secs, 0 Severely Errored Secs
     0 C-bit Unavailable Secs, 0 Path Failures
     0 Code Violations, 0 Service Affecting Secs

E1 1 is up
  timeslots:
  FDL per AT&T 54016 spec.
  No alarms detected.
  Framing is ESF, Clock Source is Internal
  Data in current interval (250 seconds elapsed):
   Near End
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
     0 Unavailable Secs, 0 Stuffed Secs
     0 Path Failures, 0 SEF/AIS Secs
   Far End
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
     0 Unavailable Secs 0 Path Failures
  Data in Interval 1:
   Near End
     0 Line Code Violations, 0 Path Code Violations
```

```
    0 Slip Secs, 2 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
    2 Errored Secs, 0 Bursty Err Secs, 2 Severely Err Secs
    0 Unavailable Secs, 0 Stuffed Secs
    1 Path Failures, 2 SEF/AIS Secs
  Far End
    0 Line Code Violations, 0 Path Code Violations
    0 Slip Secs, 2 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
    3 Errored Secs, 0 Bursty Err Secs, 3 Severely Err Secs
    0 Unavailable Secs 0 Path Failures
Total Data (last 1 15 minute intervals):
  Near End
    0 Line Code Violations,0 Path Code Violations,
    0 Slip Secs, 2 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins,
    2 Errored Secs, 0 Bursty Err Secs, 2 Severely Err Secs
    0 Unavailable Secs, 0 Stuffed Secs
    1 Path Failures, 2 SEF/AIS Secs
  Far End
    0 Line Code Violations,0 Path Code Violations
    0 Slip Secs, 2 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins,
    3 Errored Secs, 0 Bursty Err Secs, 3 Severely Err Secs
    0 Unavailable Secs, 0 Path Failures
```

Examples

show controllers ethernet

To display the hardware information specific to the Ethernet interface on Cisco 2500 and Cisco 4000 series routers, use the **showcontrollersethernet** command in user EXEC or privileged EXEC mode.

show controllers ethernet *interface-number*

Syntax Description

interface-number	Interface number of the Ethernet interface.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **showcontrollersethernet** command on Cisco 4000 series routers:

```
Router# show controllers ethernet 0
LANCE unit 0, NIM slot 1, NIM type code 4, NIM version 1
Media Type is 10BaseT, Link State is Up, Squelch is Normal
idb 0x4060, ds 0x5C80, regaddr = 0x8100000
IB at 0x600D7AC: mode=0x0000, mcfilter 0000/0001/0000/0040
station address 0000.0c03.a14f default station address 0000.0c03.a14f
buffer size 1524
RX ring with 32 entries at 0xD7E8
Rxhead = 0x600D8A0 (12582935), Rxp = 0x5CF0(23)
00 pak=0x60336D0 ds=0x6033822 status=0x80 max_size=1524 pak_size=98
01 pak=0x60327C0 ds=0x6032912 status=0x80 max_size=1524 pak_size=98
02 pak=0x6036B88 ds=0x6036CDA status=0x80 max_size=1524 pak_size=98
03 pak=0x6041138 ds=0x604128A status=0x80 max_size=1524 pak_size=98
04 pak=0x603FAA0 ds=0x603FBF2 status=0x80 max_size=1524 pak_size=98
05 pak=0x600DC50 ds=0x600DDA2 status=0x80 max_size=1524 pak_size=98
06 pak=0x6023E48 ds=0x6023F9A status=0x80 max_size=1524 pak_size=1506
07 pak=0x600E3D8 ds=0x600E52A status=0x80 max_size=1524 pak_size=1506
08 pak=0x6020990 ds=0x6020AE2 status=0x80 max_size=1524 pak_size=386
09 pak=0x602D4E8 ds=0x602D63A status=0x80 max_size=1524 pak_size=98
10 pak=0x603A7C8 ds=0x603A91A status=0x80 max_size=1524 pak_size=98
11 pak=0x601D4D8 ds=0x601D62A status=0x80 max_size=1524 pak_size=98
12 pak=0x603BE60 ds=0x603BFB2 status=0x80 max_size=1524 pak_size=98
13 pak=0x60318B0 ds=0x6031A02 status=0x80 max_size=1524 pak_size=98
14 pak=0x601CD50 ds=0x601CEA2 status=0x80 max_size=1524 pak_size=98
15 pak=0x602C5D8 ds=0x602C72A status=0x80 max_size=1524 pak_size=98
16 pak=0x60245D0 ds=0x6024722 status=0x80 max_size=1524 pak_size=98
17 pak=0x6008328 ds=0x600847A status=0x80 max_size=1524 pak_size=98
18 pak=0x601EB70 ds=0x601ECC2 status=0x80 max_size=1524 pak_size=98
19 pak=0x602DC70 ds=0x602DDC2 status=0x80 max_size=1524 pak_size=98
20 pak=0x60163E0 ds=0x6016532 status=0x80 max_size=1524 pak_size=98
21 pak=0x602CD60 ds=0x602CEB2 status=0x80 max_size=1524 pak_size=98
```

```
22 pak=0x6037A98 ds=0x6037BEA status=0x80 max_size=1524 pak_size=98
23 pak=0x602BE50 ds=0x602BFA2 status=0x80 max_size=1524 pak_size=98
24 pak=0x6018988 ds=0x6018ADA status=0x80 max_size=1524 pak_size=98
25 pak=0x6033E58 ds=0x6033FAA status=0x80 max_size=1524 pak_size=98
26 pak=0x601BE40 ds=0x601BF92 status=0x80 max_size=1524 pak_size=98
27 pak=0x6026B78 ds=0x6026CCA status=0x80 max_size=1524 pak_size=98
28 pak=0x6024D58 ds=0x6024EAA status=0x80 max_size=1524 pak_size=74
29 pak=0x602AF40 ds=0x602B092 status=0x80 max_size=1524 pak_size=98
30 pak=0x601FA80 ds=0x601FBD2 status=0x80 max_size=1524 pak_size=98
31 pak=0x6038220 ds=0x6038372 status=0x80 max_size=1524 pak_size=98
TX ring with 8 entries at 0xDA20, tx_count = 0
tx_head = 0x600DA58 (12582919), head_txp = 0x5DC4 (7)
tx_tail = 0x600DA58 (12582919), tail_txp = 0x5DC4 (7)
00 pak=0x000000 ds=0x600CF12 status=0x03 status2=0x0000 pak_size=118
01 pak=0x000000 ds=0x602126A status=0x03 status2=0x0000 pak_size=60
02 pak=0x000000 ds=0x600CF12 status=0x03 status2=0x0000 pak_size=118
03 pak=0x000000 ds=0x600CF12 status=0x03 status2=0x0000 pak_size=118
04 pak=0x000000 ds=0x600CF12 status=0x03 status2=0x0000 pak_size=118
05 pak=0x000000 ds=0x600CF12 status=0x03 status2=0x0000 pak_size=118
06 pak=0x000000 ds=0x600CF12 status=0x03 status2=0x0000 pak_size=118
07 pak=0x000000 ds=0x6003ED2 status=0x03 status2=0x0000 pak_size=126
0 missed datagrams, 0 overruns, 2 late collisions, 2 lost carrier events
0 transmitter underruns, 0 excessive collisions, 0 tdr, 0 babbles
0 memory errors, 0 spurious initialization done interrupts
0 no enp status, 0 buffer errors, 0 overflow errors
10 one_col, 10 more_col, 22 deferred, 0 tx_buff
0 throttled, 0 enabled
Lance csr0 = 0x73
Statistics:
  Rx Bytes                        58419   Tx Bytes                       17975
  Rx Good Packets                   676   Tx Good Packets                  154
  Rx Multicast                      603
  Rx Broadcast                       64
  Rx Bad Pkt Errors                   0   Tx Bad Pkt Errors                  0
  Rx FCS Errors                       0   Tx FCS Errors                      0
  Rx Runt Errors                      0   Tx Runt Errors                     0
  Rx Oversize Errors                  0   Tx Oversize Errors                 0
  Rx Length Errors                    0   Tx Collisions                      0
  Rx Code Errors                      0   Tx Late Collisions                 0
  Rx Dribble Errors                   0   Tx Excessive Collisions            0
                                          Tx Abort Errors                    0
```

The table below describes the significant fields shown in the display.

Table 52: show controllers ethernet Field Description

Field	Description
Rx Bytes	Number of packets received without any error on the interface.
Tx Bytes	Number of packets transmitted without any error on the interface.
Rx Good Packets	Number of packets received without any error on the interface.
Tx Good Packets	Number of packets transmitted without any error on the interface.
Rx Multicast	Number of multicast packets received on the interface.
Rx Broadcast	Number of broadcast packets received on the interface.
Rx Bad Pkt Errors	Number of bad frames received on the interface.

Field	Description
Rx FCS Errors	Number of valid size frames with Frame Check Sequence (FCS) errors, but not with framing errors.
Rx Runt Errors	Frames received on the interface that are smaller than the minimum IEEE 802.3 frame size (64 bytes for Ethernet).
Rx Oversize Errors	Number of oversize packets received on the interface.
Rx Length Errors	Number of packets received on the interface with errors in the length of the packet.
Tx Collisions	Number of collision events on the interface. This is applicable only in the half-duplex mode.
Rx Code Errors	Number of packets received on the interface with the code error signal.
Tx Late Collisions	Number of late collisions.
Rx Dribble Errors	Number of packets received with the dribble error. When a packet does not contain an integral number of bytes, it is a dribble error .
Excessive Collisions	Number of frames dropped in the transmit direction due to excessive collision. This is applicable only in the half-duplex mode.
Tx Abort Errors	Number of packets that were aborted during transmission.

Related Commands

Command	Description
show controllers	Displays information specific to the hardware on a line card.

show controllers fastethernet

To display information about initialization block, transmit ring, receive ring, Fast Ethernet interface information, applicable MAC destination address and VLAN filtering tables, and errors for the Fast Ethernet controller chip, use the **showcontrollersfastethernet** command in user EXEC or privileged EXEC mode.

Standard Syntax

show controllers fastethernet *number*

Cisco 7200 Series

show controllers fastethernet *slot/port*

Cisco 7500 Series

show controllers fastethernet *slot/port-adaptor/port*

Shared Port Adapter

show controllers fastethernet *slot/sub-slot/port*{[**detail**]}

Syntax Description

number	Port, connector, or interface card number. On a Cisco 4500 or Cisco 4700 router, specifies the network processor module (NPM) number. The numbers are assigned at the factory at the time of installation or when added to a system.
slot	Slot number. Refer to the appropriate hardware manual for slot information.
/ *port*	Port number. Refer to the appropriate hardware manual for port information.
/ *port-adapter*	Port adapter number. Refer to the appropriate hardware manual for information about port adapter compatibility.
subslot	(Optional) Secondary slot number on a jacket card where a SPA is installed.
detail	Specifies display of additional low-level diagnostic information.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
11.2	This command was introduced.
12.2S	This command was integrated into Cisco IOS Release 12.2S.
12.2(20)S2	This command was implemented on the 4-Port 10/100 Fast Ethernet SPA on the Cisco 7304 router and introduced a new address format and output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The output from this command is generally useful for diagnostic tasks performed by technical support.

Shared Port Adapter Usage Guidelines

The output from the **showcontrollersfastethernet**command for the 4-Port 10/100 Fast Ethernet SPA provides several different sections of information and statistics that are organized according to the internal hardware devices and the various paths in the flow of data on the SPA. The following sections are provided:

Several areas of the output are generally useful for diagnostic tasks performed by Cisco Systems technical support personnel only.

Examples

The following is a sample output from the **showcontrollersfastethernet** command on a Cisco 4500 series router:

```
Router# show controllers fastethernet 0
DEC21140 Slot 0, Subunit 0
dec21140_ds=0x60001234, registers=0x3c001000, ib=0x42301563, ring entries=256
rxring=0x40235878, rxr shadow=0x64528745, rx_head=0, rx_tail=10
txring=0x43562188, txr shadow=0x65438721, tx_head=17, tx_tail=34, tx_count=17
DEC21140 Registers
CSR0=0x23457667, CSR3=0x12349878, CSR4=0x34528745, CSR5=0x76674565
CSR6=0x76453676, CSR7=0x76456574, CSR8=0x25367648, CSR9=0x87253674
CSR11=0x23456454, CSR12=0x76564787, CSR15=0x98273465
DEC21140 PCI registers
bus_no=0, device_no=0
CFID=0x12341234, CFCS=0x76547654, CFRV=0x87658765, CFLT=0x98769876
CBIO=0x12344321, CBMA=0x23454321, CFIT=0x34567654, CFDA=0x76544567
MII registers
Register 0x00: 0x1234 0x1234 0x2345 0x3456 0x4567 0x5678 0x6789 0x7890
Register 0x08: 0x9876 0x8765 0x7654 0x6543 0x5432 0x4321 0x3210 0x2109
Register 0x10: 0x1234 0x2345 0x3456            0x4567 0x5678 0x6789 0x7890
Register 0x18: 0x9876 0x8765 0x7654 0x6543 0x5432 0x4321
DEC21140 statistics
filtered_in_sw=1000, throttled=10, enabled=10
rx_fifo_overflow=10, rx_no_enp=12, rx_late_collision=18
rx_watchdog=15, rx_process_stopped=15, rx_buffer_unavailable=1500
tx_jabber_timeout=10, tx_carrier_loss=2, tx_deffered=15
tx_no_carrier=1, tx_late_collision=10, tx_excess_coll=10
tx_process_stopped=1, fata_tx_err=0
```

The following is a sample output from the **showcontrollersfastethernet** command on a Cisco AS5300 router:

```
Router# show controller fastethernet 0
DEC21140
Setup Frame
 (0 ) 00e0.1e3e.c179
 (1 ) 0100.0ccc.cccc
 (2 ) 0900.2b00.000f
 (3 ) 0900.2b02.0104
 (4 ) 0300.0000.0001
 dec21140_ds=0x60BD33B8, registers=0x3C210000, ib=0x4002F75C, ring entries=32
 rxring=0x4002F844, rxr shadow=0x60F14B58, rx_head=6, rx_tail=6
 txring=0x4002FA6C, txr shadow=0x60F14BF8, tx_head=10, tx_tail=10, tx_count=0
```

```
 tx_size=32, rx_size=32
 PHY link up
 DEC21140 Registers:
 CSR0=0xFE024480, CSR3=0x4002F844, CSR4=0x4002FA6C, CSR5=0xFC660000
 CSR6=0x322C2002, CSR7=0xFFFFA241, CSR8=0xE0000000, CSR9=0xFFFDC3FF
 CSR11=0xFFFE0000, CSR12=0xFFFFFF09, CSR15=0xFFFFFEC8
 DEC21140 PCI registers:
  bus_no=2, device_no=0
  CFID=0x00091011, CFCS=0x82800005, CFRV=0x02000021, CFLT=0x0000FF00
  CBIO=0x3C210001, CBMA=0x00000000, CFIT=0x28140100, CFDA=0x00000000
 MII registers:
  Register 0x00:   0000  784D  2000  5C01  0001  0000  0000  0000
  Register 0x08:   0000  0000  0000  0000  0000  0000  0000  0000
  Register 0x10:   0000  0000  0000  0000        0000  0001  8060
  Register 0x18:   8020  0840  0000  3000  A3B9
 throttled=7, enabled=7
 rx_fifo_overflow=0, rx_no_enp=0, late_collision=0
 rx_watchdog=0, rx_process_stopped=0, rx_buffer_unavailable=0
 tx_jabber_timeout=0, tx_carrier_loss=1, tx_deferred=0
 tx_no_carrier=1, tx_late_collision=0, tx_excess_coll=0
 tx_process_stopped=0, fatal_tx_err=0
 overflow_resets=0
0 missed datagrams, 0 overruns
0 transmitter underruns, 0 excessive collisions
0 single collisions, 0 multiple collisions
0 dma memory errors, 0 CRC errors
0 alignment errors, 0 runts, 0 giants
```

The following is a sample output from the **showcontrollersfastethernet** command on a Cisco 7200 series router:

```
Router# show controllers fastethernet 0/0
Interface Fast Ethernet0/0
Hardware is DEC21140
 dec21140_ds=0x60895888, registers=0x3C018000, ib=0x4B019500
 rx ring entries=128, tx ring entries=128
 rxring=0x4B019640, rxr shadow=0x60895970, rx_head=0, rx_tail=0
 txring=0x4B019EC0, txr shadow=0x60895B98, tx_head=77, tx_tail=77, tx_count=0
 CSR0=0xFFFA4882, CSR3=0x4B019640, CSR4=0x4B019EC0, CSR5=0xFC660000
 CSR6=0xE20CA202, CSR7=0xFFFFA241, CSR8=0xFFFE0000, CSR9=0xFFFDD7FF
 CSR11=0xFFFE0000, CSR12=0xFFFFFF98, CSR15=0xFFFFFEC8
 DEC21140 PCI registers:
  bus_no=0, device_no=6
  CFID=0x00091011, CFCS=0x02800006, CFRV=0x02000012, CFLT=0x0000FF00
  CBIO=0x7C5AFF81, CBMA=0x48018000, CFIT=0x0000018F, CFDA=0x0000AF00
 MII registers:
  Register 0x00:   2000  780B  2000  5C00  01E1  0000  0000  0000
  Register 0x08:   0000  0000  0000  0000  0000  0000  0000  0000
  Register 0x10:   0000  0000  0000  0000        0000  0000  8040
  Register 0x18:   8000  0000  0000  3800  A3B9
 throttled=0, enabled=0, disabled=0
 rx_fifo_overflow=0, rx_no_enp=0, rx_discard=0
 tx_underrun_err=0, tx_jabber_timeout=0, tx_carrier_loss=1
 tx_no_carrier=1, tx_late_collision=0, tx_excess_coll=0
 tx_collision_cnt=0, tx_deferred=0, fatal_tx_err=0, mult_ovfl=0
HW addr filter: 0x60895FC0, ISL Enabled
  Entry= 0: Addr=0100.0CCC.CCCC
  Entry= 1: Addr=0300.0000.0001
  Entry= 2: Addr=0100.0C00.0000
  Entry= 3: Addr=FFFF.FFFF.FFFF
  Entry= 4: Addr=FFFF.FFFF.FFFF
  Entry= 5: Addr=FFFF.FFFF.FFFF
  Entry= 6: Addr=FFFF.FFFF.FFFF
```

```
  Entry= 7: Addr=FFFF.FFFF.FFFF
  Entry= 8: Addr=FFFF.FFFF.FFFF
  Entry= 9: Addr=FFFF.FFFF.FFFF
  Entry=10: Addr=FFFF.FFFF.FFFF
  Entry=11: Addr=FFFF.FFFF.FFFF
  Entry=12: Addr=FFFF.FFFF.FFFF
  Entry=13: Addr=FFFF.FFFF.FFFF
  Entry=14: Addr=FFFF.FFFF.FFFF
  Entry=15: Addr=0060.3E28.6E00
```

Shared Port Adapter Examples

The following is sample output from the **showcontrollersfastethernet** command for the first interface (port 0) on a 4-Port 10/100 Fast Ethernet SPA that is located in the top subslot (0), of the MSC that is installed in slot 4 on a Cisco 7304 router:

```
Router# show controllers fastethernet 4/0/0
Interface FastEthernet4/0/0
  Hardware is SPA-4FE-7304
  Connection mode is auto-negotiation
  Interface state is up, link is up
  Configuration is Auto Speed, Auto Duplex
  Selected media-type is RJ45
  Promiscuous mode is off, VLAN filtering is enabled
  MDI crossover status: MDI
  Auto-negotiation configuration and status:
    Auto-negotiation is enabled and is completed
    Speed/duplex is resolved to 100 Mbps, full duplex
    Advertised capabilities: 10M/HD 10M/FD 100M/HD 100M/FD Pause capable (Asymmetric)
    Partner capabilities: 10M/HD 10M/FD 100M/HD 100M/FD Pause capable
MAC counters:
  Input: packets = 15, bytes = 1776
         FIFO full/reset removed = 0, error drop = 0
  Output: packets = 18, bytes = 2622
          FIFO full/reset removed = 0, error drop = 0
  Total pause frames: transmitted = 0, received = 0
FPGA counters:
  Input: Total (good & bad) packets: 15, TCAM drops: 4
         Satisfy (host-backpressure) drops: 0, CRC drops: 0
         PL3 RERRs: 0
  Output: EOP (SPI4) errors: 0
SPA carrier card counters:
  Input: packets = 11, bytes = 1476, drops = 0
  Output: packets = 18, bytes = 2550, drops = 0
  Egress flow control status: XON
  Per bay counters:
  General errors: input = 0, output = 0
  SPI4 errors: ingress dip4 = 0, egress dip2 = 0
SPA Error counters:
  SPI4 TX out of frame error = 2 (00:02:31 ago)
  SPI4 TX Train valid error = 1 (00:02:11 ago)
  SPI4 TX DIP4 error = 1 (00:01:30 ago)
  SPI4 RX out of frame error = 1 (00:00:36 ago)
  SPI4 RX DIP2 error = 1 (00:00:13 ago)
MAC destination address filtering table:
  Table entries: Total = 512, Used = 4, Available = 508
  Index MAC destination address       Mask
  ----- ----------------------  --------------
  1     0007.0ed3.ba80           ffff.ffff.ffff
  2     ffff.ffff.ffff           ffff.ffff.ffff
  3     0100.0000.0000           0100.0000.0000
```

```
  4     0100.0ccc.cccc           ffff.ffff.ffff
VLAN filtering table:
  Number of VLANs configured on this interface = 0
  Table entries: Total = 1024, Used = 2, Available = 1022
  Index  VLAN identifier  Enabled  Tunnel
  -----  ---------------  -------  ------
  1           0             No      No
  2           0             Yes     No
Platform details:
  PXF tif number: 0x10
```

The table below describes the fields shown in the interface configuration section of the display. This section is useful for verifying the status of autonegotiation and configured parameters on the link, and the amount of traffic being handled by the interface.

Table 53: show controllers Command Field Descriptions--Interface Section

Field	Description
Interface	Name of the interface.
Hardware	Type of hardware.
Connection mode	Indicator of autonegotiation used to establish the connection.
Link	State of the link.
Configuration	Configuration of the speed and duplex operation on the interface.
Selected media-type	Interface port media type. RJ-45 is the only type supported on the 4-Port 10/100 Fast Ethernet SPA.
Promiscuous mode	State of promiscuous mode (on or off). When promiscuous mode is on, the SPA disables MAC destination address and VLAN filtering. When promiscuous mode is off, the SPA enables MAC destination address and VLAN filtering.
VLAN filtering	Status of ternary content addressable memory (TCAM) filtering of VLANs (enabled or disabled). By default, the SPA always enables VLAN filtering. The SPA disables VLAN filtering if the TCAM table is full, or if the SPA is operating in promiscuous mode. **Note** VLAN filtering is not enabled or disabled using any command-line interface (CLI) command.
MDI crossover status	State of the media dependent interface (MDI) for the PHY device on the specified interface. The possible values are MDI for straight-through cables or media dependent interface crossover (MDI-X) for crossover cables.
Auto-negotiation	State of autonegotiation (enabled or disabled) on the interface and its current status.
Speed/duplex is resolved to	Results of autonegotiated parameter values (speed and duplex) currently being used on the link.

Field	Description
Advertised capabilities	List of the possible combinations of speed and duplex modes (in *speed*/*duplex* format) and flow control that the local interface has advertised it supports to the remote device: • For speed--10M is 10 Mbps, and 100M is 100 Mbps. • For duplex--HD is half duplex, and FD is full duplex. • For flow control--"Pause capable (Asymmetric)" means that the SPA advertises support of the PAUSE flow control bit and the ASM_DIR (asymmetric) flow control bit.
Partner capabilities	List of the possible combinations of speed and duplex modes (in *speed*/*duplex* format) and flow control that the remote device has advertised it supports to the local interface: • For speed--10M is 10 Mbps, and 100M is 100 Mbps. • For duplex--HD is half duplex, and FD is full duplex. • For flow control--"Pause capable" means that the remote device supports implementation of the PAUSE flow control bit; "Pause capable (Asymmetric)" means that the remote device supports implementation of the PAUSE flow control bit and the ASM_DIR (asymmetric) flow control bit.

The table below describes the fields shown in the MAC counters section of the display. This section is useful for verifying the status of packets processed by the MAC device for the interface. This information is useful for Cisco Systems technical support personnel.

Table 54: show controllers Command Field Descriptions--MAC Counters Section

Field	Description
Input: packets, bytes	Total number of packets and bytes received by the MAC device for the interface since it was activated or cleared. You can clear these counters using the **clearcounters** privileged EXEC command.
Input: FIFO full/reset removed	Total number of packets removed by the MAC device due to a first-in, first-out (FIFO) overflow condition in the input buffer for the interface.
Input: error drop	Total number of input packets with errors that are dropped by the MAC device for the interface.
Output: packets, bytes	Total number of packets and bytes transmitted by the MAC device for the interface since it was activated or cleared. You can clear these counters using the **clearcounters** privileged EXEC command.

Field	Description
Output: FIFO full/reset removed	Total number of packets removed by the MAC device due to a first-in, first-out (FIFO) overflow condition in the output buffer for the interface.
Output: error drop	Total number of output packets with errors that are dropped by the MAC device for the interface.
Total pause frames	Total number of Ethernet 802.3x pause frames transmitted and received by the MAC device for flow control on the interface.

The table below describes the fields shown in the FPGA counters section of the display. This section is useful for verifying the status of packets processed by the FPGA device for the interface. This information is useful for Cisco Systems technical support personnel.

Table 55: show controllers Command Field Descriptions--FPGA Counters Section

Field	Description
Input: Total (good & bad) packets	Total number of packets received by the FPGA device in the ingress direction for the interface.
Input: TCAM drops	Total number of packets dropped by the FPGA device in the ingress direction for the interface due to a ternary content addressable memory (TCAM) lookup failure. This counter increments when the interface receives a frame with a destination MAC address or VLAN identifier that is not present in the TCAM table.
Input: Satisfy (host-backpressure) drops	Total number of packets dropped by the FPGA device in the ingress direction for the interface due to back-pressure from the MSC.
Input: CRC drops	Total number of packets dropped by the FPGA device in the ingress direction for the interface due to cyclic redundancy check (CRC) errors.
Input: PL3 RERRs	Total number of packets with errors received for the interface by the FPGA device in the ingress direction over the System Packet Interface Level 3 (SPI3) (also called PL3) path from the MAC device to the FPGA device.
Output: EOP (SPI4) errors	Total number of packets with end-of-packet (EOP) errors received by the FPGA device in the egress direction for the interface over the System Packet Interface Level 4 (SPI4) path from the MSC to the FPGA device.

The table below describes the fields shown in the SPA carrier card counters section of the display. This section is useful for verifying the status of packets processed by the MSC for the interface. This information is useful for Cisco Systems technical support personnel.

Table 56: show controllers Command Field Descriptions--SPA Carrier Card Counters Section

Field	Description
Input: packets, bytes, drops	Total number of packets, bytes, and packet drops that have occurred on the SPI4 path from the FPGA device to the MSC.

Field	Description
Output: packets, bytes, drops	Total number of packets, bytes, and packet drops that have occurred on the SPI4 path from the MSC to the FPGA device.
Egress flow control status	Status of flow control between the MSC and the Route Processor (RP). The possible values are: • XON--A control frame has been sent by the MSC to the RP to indicate that the MSC is ready to accept data. • XOFF--A control frame has been sent by the MSC to the RP to indicate congestion on the MSC. The MSC cannot accept any more data from the RP during this condition.
General errors	Total number of errors (such as parity) on the MSC in the ingress and egress direction.
SPI4 errors: ingress dip4	Total number of 4-bit Diagonal Interleaved Parity (DIP4) errors in the ingress direction on the SPI4 path from the FPGA device to the MSC. DIP4 is a parity algorithm where a 4-bit odd parity is computed diagonally over control and data words.
SPI4 errors: egress dip2	Total number of 2-bit Diagonal Interleaved Parity (DIP2) errors in the egress direction on the SPI4 path from the FPGA device to the MSC. DIP2 is a parity algorithm where a 2-bit odd parity is computed diagonally over status words.

The table below describes the fields shown in the SPA error counters section of the display. This section appears only when one of the SPI4 transmit or receive errors occurs on the interface. This information is useful for Cisco Systems technical support personnel.

Note None of the SPA SPI4 error counters appear in **showcontrollersfastethernet** command output until at least one of those types of SPI4 errors occurs.

All of the errors in the SPA error counters section are subject to the SPA automatic recovery process when certain thresholds are reached. For more information about this process on the Cisco 7304 router, refer to the “Understanding SPA Automatic Recovery” section of the *Cisco 7304 Router Modular Services Card and Shared Port Adapter Software Configuration Guide*

Table 57: show controllers Command Field Descriptions--SPA Error Counters Section

Field	Description
SPI4 TX out of frame error = 2 (00:02:31 ago)	Number of SPI4 out-of-frame errors (events) detected in the transmit direction (toward the network), from the MSC to the SPA FPGA device. The time stamp indicates how long ago (in hours:minutes:seconds) from the current system time, that the last error was detected. This error indicates a loss of synchronization between the synchronization block and the data received on the SPI4 path. When synchronization is reacquired, the error no longer occurs.
SPI4 TX Train valid error = 1 (00:02:11 ago)	Number of times that a low-level synchronization problem was detected in the transmit direction (toward the network), from the MSC to the SPA FPGA device. The time stamp indicates how long ago (in hours:minutes:seconds) from the current system time, that the last error was detected.
SPI4 TX DIP4 error = 1 (00:01:30 ago)	Number of 4-bit Diagonal Interleaved Parity (DIP4) errors in the transmit direction (toward the network), from the MSC to the SPA FPGA device. The time stamp indicates how long ago (in hours:minutes:seconds) from the current system time, that the last error was detected. DIP4 is a parity algorithm where a 4-bit odd parity is computed diagonally over control and data words.
SPI4 RX out of frame error = 1 (00:00:36 ago)	Number of SPI4 out-of-frame errors (events) detected in the receive direction (from the network), from the SPA FPGA device to the MSC. The time stamp indicates how long ago (in hours:minutes:seconds) from the current system time, that the last error was detected. This error indicates a loss of synchronization between the synchronization block and the data received on the SPI4 path. When synchronization is reacquired, the error no longer occurs.
SPI4 RX DIP2 error = 1 (00:00:13 ago)	Number of 2-bit Diagonal Interleaved Parity (DIP2) errors in the receive direction (from the network), from the SPA FPGA device to the MSC. The time stamp indicates how long ago (in hours:minutes:seconds) from the current system time, that the last error was detected. DIP2 is a parity algorithm where a 2-bit odd parity is computed diagonally over status words.

The table below describes the fields shown in the MAC destination address filtering table section of the display. This section is useful for verifying the multicast destination addresses that are in the TCAM table and permitted by the interface. This information is useful for Cisco Systems technical support personnel.

Table 58: show controllers Command Field Descriptions--MAC Destination Address Filtering Table Section

Field	Description
Table entries: Total, Used, Available	Total number of MAC destination address entries possible in the TCAM table for the interface, the number of table entries currently used by the interface, and the number of table entries that remain available. The 4-Port 10/100 Fast Ethernet SPA supports a 512-entry MAC filtering table for each supported interface (2048 entries total on the card).
Index	Table entry identifier.
MAC destination address	MAC destination address (multicast) permitted by the interface and used in the TCAM lookup table for packet filtering. The multicast MAC entries typically come from routing protocols [such as Open Shortest Path First (OSPF) and Enhanced IGRP (EIGRP)], and other protocols including the Hot Standby Router Protocol (HSRP). When the router reloads, three addresses appear by default in the MAC filtering table: the unicast address of the local interface, the Ethernet broadcast address, and the Ethernet multicast address.
Mask	Mask for the corresponding destination address. The SPA uses the bits that are set in the mask to look up the address in the TCAM table.

The table below describes the fields shown in the VLAN filtering table section of the display. This section is useful for verifying the VLANs that are in the TCAM table and are permitted by the interface. This information is useful for Cisco Systems technical support personnel.

Table 59: show controllers Command Field Descriptions--VLAN Filtering Table Section

Field	Description
Number of VLANs configured on this interface	Number of VLANs that are configured on the interface. If the number of VLANs configured on the interface is 1022 or less, then the VLAN filtering table also shows an index entry for every VLAN ID. The number of VLANs configured on the interface can be 0, while the number of used table entries reports 2, because the SPA always uses two entries to provide valid matching criteria for promiscuous mode and non-VLAN packets.
Table entries: Total, Used, Available	Total number of VLAN entries possible in the TCAM filtering table for the interface, the number of table entries currently used by the interface (two are always in use by default), and the number of table entries that remain available. The 4-Port 10/100 Fast Ethernet SPA supports a 1024-entry VLAN filtering table for each supported interface (4096 entries total on the card).
Index	Table entry identifier.
VLAN identifier	Number of the VLAN. Two VLAN ID 0 entries always appear in the table and represent the local interface port for handling of promiscuous mode and non-VLAN packets. Other VLAN entries appear in this table when VLANs are configured on the interface.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Enabled</td><td>Status of the VLAN ID for TCAM filtering, with the following possible values:
• No--The entry is disabled for filtering.
• Yes--The entry is enabled for filtering.

The TCAM filter uses the “first-match” rule to filter packets that the SPA receives against entries in the table. The matching assessment begins at the top of the table with the VLAN ID 0 entries.

Note The SPA always supports two VLAN ID 0 entries. The first VLAN ID 0 entry of the TCAM table is used for promiscuous mode. It has a value of “No,” meaning it is disabled, whenever promiscuous mode is disabled for the interface. The second VLAN ID 0 entry is used for filtering of non-VLAN packets.</td></tr>
<tr><td>Tunnel</td><td>Status of tunneling for the interface, with the following possible values:
• No--Tunneling is disabled and the SPA performs MAC destination address filtering.
• Yes--Tunneling is enabled and the SPA does not perform MAC destination address filtering.

Note If promiscuous mode is enabled, then the first VLAN ID 0 entry shows tunnel = Yes. All other VLAN ID entries show tunnel = No.</td></tr>
</table>

The table below describes the fields shown in the Platform details section of the display.

Table 60: show controllers Command Field Descriptions--Platform Details Section

Field	Description
PXF tif number	Number of the interface (in hexadecimal format) used for PXF on the network services engine (NSE) or by the Hyper Transport (HT) FPGA device on the network processing engine (NPE).

Related Commands

Command	Description
show interfaces fastethernet	Displays information about the Fast Ethernet interfaces.

show controllers fddi

To display all information under the FDDI Interface Processor (FIP) on the Cisco 7200 series and Cisco 7500 series routers, use the **showcontrollersfddi** command in user EXEC or privileged EXEC mode.

show controllers fddi

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command reflects the internal state of the chips and information that the system uses for bridging and routing that is specific to the interface hardware. The information displayed is generally useful for diagnostic tasks performed by technical support personnel only.

Examples

The following is sample output from the **showcontrollersfddi** command:

```
Router# show controllers fddi
Fddi2/0 - hardware version 2.2, microcode version 1.2
  Phy-A registers:
    cr0 4, cr1 0, cr2 0, status 3, cr3 0
  Phy-B registers:
    cr0 4, cr1 4, cr2 0, status 3, cr3 0
  FORMAC registers:
    irdtlb  71C2, irdtneg F85E, irdthtt F5D5, irdmir  FFFF0BDC
    irdtrth F85F, irdtmax FBC5, irdtvxt 5959, irdstmc 0810
    irdmode 6A20, irdimsk 0000, irdstat 8060, irdtpri 0000
  FIP registers
    ccb:   002C  cmd:   0006  fr:   000F  mdptr: 0000  mema: 0000
    icb:   00C0  arg:   0003  app:  0004  mdpg:  0000  af:   0603
    clm:   E002  bcn:   E016  clbn: 0198  rxoff: 002A  en:   0001
    clmbc: 8011  bcnbc: 8011  robn: 0004  park:  0000  fop:  8004
    txchn: 0000  pend:  0000  act:  0000  tail:  0000  cnt:  0000
    state: 0003  check: 0000  eof:  0000  tail:  0000  cnt:  0000
    rxchn: 0000  buf0:  0534  nxt0: 0570  eof:   0000  tail: 0000
    eofch: 0000  buf1:  051C  nxt1: 0528  pool:  0050  err:  005C
    head:  0984  cur:   0000  t0:   0030  t1:    0027  t2:   000F
    tail:  0984  cnt:   0001  t3:   0000  rxlft: 000B  used: 0000
    txq_s: 0018  txq_f: 0018  Aarm: 0000  Barm:  1388  fint: 8004
 Total LEM: phy-a 6, phy-b 13
```

The last line of output indicates how many times the specific PHY encountered an “UNKNOWN LINE STATE” event on the fiber.

show controllers gigabitethernet

To display initialization block information, transmit ring, receive ring, transmission statistics and errors, and applicable MAC destination address and VLAN filtering tables for Gigabit Ethernet interface controllers, use the **showcontrollersgigabitethernet**command in privileged EXEC mode.

Standard Syntax

show controllers gigabitethernet *slot*/*port*

Shared Port Adapters

show controllers gigabitethernet *slot*/*subslot*/*port* [**detail**]

Syntax Description

slot	(Optional) Chassis slot number. Refer to the appropriate hardware manual for slot information. For MSCs, refer to the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for MSCs and SPAs" topic in the platform-specific SPA software configuration guide.
/ *subslot*	(Optional) Secondary slot number on a MSC where a SPA is installed. Refer to the platform-specific SPA hardware installation guide and the corresponding "Specifying the Interface Address on a SPA" topic in the platform-specific SPA software configuration guide for subslot information.
/ *port*	(Optional) Port or interface number. Refer to the appropriate hardware manual for port information. For SPAs, refer to the corresponding "Specifying the Interface Address on a SPA" topics in the platform-specific SPA software configuration guide.
detail	Specifies display of additional low-level diagnostic information.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1CC	This command was introduced.
12.1(3a)E	Support for the Cisco 7200-I/O-GE+E controller was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2S	This command was integrated into Cisco IOS Release 12.2S.
12.2(20)S2	This command was implemented on the 2-Port 10/100/1000 Gigabit Ethernet SPA on the Cisco 7304 router with a new address format and output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.2(02)SA	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

This command is used to display hardware and software information about the Gigabit Ethernet interface. The I/O controller is always found in slot 0.

Shared Port Adapter Usage Guidelines

The output from the **showcontrollersgigabitethernet**command for the 2-Port 10/100/1000 Gigabit Ethernet SPA provides several different sections of information and statistics that are organized according to the internal hardware devices and the various paths in the flow of data on the SPA. Several areas of the output are generally useful for diagnostic tasks performed by technical support only.

Examples

The following is sample output from the **showcontrollersgigabitethernet**command:

```
Router# show controllers gigabitethernet 0/0
Interface GigabitEthernet0/0 (idb 0x627D8344)
Hardware is i82543 (Livengood) A1
network connection mode is AUTO
network link is up
loopback type is none
SERDES is enabled (TBI mode), GBIC is enabled
GBIC type is 1000BaseSX
idb->lc_ip_turbo_fs=0x604A82B0, ip_routecache=0x1(dfs=0/mdfs=0), max_mtu=1524
i82543_ds=0x627DA094, registers=0x3C100000, curr_intr=0
rx cache size=2000, rx cache end=1744, rx_nobuffer=0
i82543 MAC registers:
CTRL  =0x0ACC0004, STATUS=0x00000FAB, CTRL_X=0x000048E0, IMS   =0x00000096
RCTL  =0x0042803A, RDBAL =0x2000E000, RDBAH =0x00000000, RDLEN =0x00001000
RDH   =0x000000CB, RDT   =0x000000CA, RDTR  =0x00000000
TCTL  =0x000400FA, TDBAL =0x20010000, TDBAH =0x00000000, TDLEN =0x00001000
TDH   =0x00000057, TDT   =0x00000057, TIPG  =0x00600806
ETT   =0x00000000, TXDMAC=0x00000001
TXCW  =0xC00001A0, RXCW  =0xDC004120, FCRTH =0x0000AFF0, FCRTL =0x80001200
FCAH  =0x00000100, FCAL  =0x00C28001, FCT   =0x00008808, FCTTV =0x00000080
RDFH  =0x00000BFA, RDFT  =0x00000BFA, RDFPC =0x00000000
TDFH  =0x00001EBA, TDFT  =0x00001EBA, TDFPC =0x00000000
RX is normal, enabled  TX is normal, enabled
Device status = full-duplex, link up
AN status = done(RF:0 , PAUSE:2 ), bit sync OK, rx idle stream, rx invalid
symbols, rx idle char
GBIC registers:
Register 0x00:  01  00  01  00  00  00  01  00
Register 0x08:  00  00  00  00  0D  00  00  00
Register 0x10:  32  1E  00  00  4D  65  74  68
Register 0x18:  6F  64  65  20  45  6C  65  63
Register 0x20:  2E  20  20  20  00  00  00  00
Register 0x28:  4D  47  42  43  2D  32  30  2D
Register 0x30:  34  2D  31  2D  53  20  20  20
Register 0x38:  31  30  30  30  00  00  00  55
Register 0x40:  00  0A  00  00  41  4A  42  48
Register 0x48:  47  30  36  30  20  20  20  20
Register 0x50:  20  20  20  20  30  30  30  33
Register 0x58:  32  30  20  20  00  00  00  61
PartNumber:MGBC-20-4-1-S
```

```
PartRev:G
SerialNo:AJBHG060
Options: 0
Length(9um/50um/62.5um):000/500/300
Date Code:000320
Gigabit Ethernet Codes: 1
PCI configuration registers:
bus_no=0, device_no=8
DeviceID=0x1001, VendorID=0x8086, Command=0x0156, Status=0x0230
Class=0x02/0x00/0x00, Revision=0x01, LatencyTimer=0xFC, CacheLineSize=0x20
BaseAddr0=0x48100000, BaseAddr1=0x00000000, MaxLat=0x00, MinGnt=0xFF
SubsysDeviceID=0x1001, SubsysVendorID=0x8086
Cap_Ptr=0x000000DC  Retry/TRDY Timeout=0x00000000
PMC=0x00220001  PMCSR=0x00000000
I82543 Internal Driver Variables:
rxring(256)=0x2000E000, shadow=0x627DA3F0, head=203, rx_buf_size=512
txring(256)=0x20010000, shadow=0x627DA81C, head=87, tail=87
chip_state=2, pci_rev=1
tx_count=0, tx_limited=0
rx_overrun=0, rx_seq=0, rx_no_enp=0, rx_discard=0
throttled=0, enabled=0, disabled=0
reset=17(init=1, check=0, restart=3, pci=0), auto_restart=18
link_reset=0, tx_carrier_loss=1, fatal_tx_err=0
isl_err=0, wait_for_last_tdt=0
HW addr filter:0x627DB048, ISL disabled, Promiscuous mode on
Entry= 0: Addr=0000.C000.4000
(All other entries are empty)
i82543 Statistics
CRC error        0             Symbol error     7
Missed Packets   0             Single Collision 0
Excessive Coll   0             Multiple Coll    0
Late Coll        0             Collision        0
Defer            0             Receive Length   0
Sequence Error   0             XON RX           0
XON TX           0             XOFF RX          0
OFF TX          0             FC RX Unsupport  0
Packet RX (64)   11510         Packet RX (127)  17488
Packet RX (255)  1176          Packet RX (511)  7941
Packet RX (1023) 738           Packet RX (1522) 18
Good Packet RX   38871         Broadcast RX     0
Multicast RX     0             Good Packet TX   5208
Good Octets RX.H 0             Good Octets RX.L 5579526
Good Octets TX.H 0             Good Octets TX.L 513145
RX No Buff       0             RX Undersize     0
RX Fragment      0             RX Oversize      0
RX Octets High   0             RX Octets Low    5579526
TX Octets High   0             TX Octets Low    513145
TX Packet        5208          RX Packet        38871
TX Broadcast     1796          TX Multicast     330
Packet TX (64)   1795          Packet TX (127)  3110
Packet TX (255)  0             Packet TX (511)  300
Packet TX (1023) 3             Packet TX (1522) 0
TX Underruns     0             TX No CSR        0
RX Error Count   0             RX DMA Underruns 0
RX Carrier Ext   0
TCP Segmentation 0             TCP Seg Failed   0
```

Shared Port Adapter Examples

The following is sample output from the **showcontrollersgigabitethernet** command for the first RJ-45 interface (port 0) in a 2-Port 10/100/1000 Gigabit Ethernet SPA located in the top subslot (0) of the MSC that is installed in slot 5 on a Cisco 7304 router. This output also shows the SPA Error counters section that appears only if one of the types of SPI4 errors occurs on the interface:

```
Router#  show controllers gigabitethernet 0/0
Interface GigabitEthernet5/0/0
  Hardware is SPA-2GE-7304
  Connection mode is auto-negotiation
  Interface state is up, link is up
  Configuration is Auto Speed, Auto Duplex
  Selected media-type is RJ45
  Promiscuous mode is off, VLAN filtering is enabled
  MDI crossover status: MDIX
  Auto-negotiation configuration and status:
    Auto-negotiation is enabled and is completed
    Speed/duplex is resolved to 1000 Mbps, full duplex
    Advertised capabilities: 10M/HD 10M/FD 100M/HD 100M/FD 1000M/HD 1000M/FD
                             Pause capable (Asymmetric)
    Partner capabilities: 10M/HD 10M/FD 100M/HD 100M/FD 1000M/FD Pause capable
MAC counters:
  Input: packets = 0, bytes = 0
         FIFO full/reset removed = 0, error drop = 0
  Output: packets = 1, bytes = 64
          FIFO full/reset removed = 0, error drop = 0
  Total pause frames: transmitted = 0, received = 0
FPGA counters:
  Input: Total (good & bad) packets: 0, TCAM drops: 0
         Satisfy (host-backpressure) drops: 0, CRC drops: 0
         PL3 RERRs: 0
  Output: EOP (SPI4) errors: 0
SPA carrier card counters:
  Input: packets = 0, bytes = 0, drops = 0
  Output: packets = 1, bytes = 60, drops = 0
  Egress flow control status: XON
  Per bay counters:
  General errors: input = 0, output = 0
  SPI4 errors: ingress dip4 = 0, egress dip2 = 0
SPA Error counters:
  SPI4 TX out of frame error = 2 (00:02:31 ago)
  SPI4 TX Train valid error = 1 (00:02:11 ago)
  SPI4 TX DIP4 error = 1 (00:01:30 ago)
  SPI4 RX out of frame error = 1 (00:00:36 ago)
  SPI4 RX DIP2 error = 1 (00:00:13 ago)
MAC destination address filtering table:
  Table entries: Total = 1024, Used = 3, Available = 1021
  Index MAC destination address       Mask
  ----- -----------------------  --------------
  1     00b0.64ff.5aa0           ffff.ffff.ffff
  2     ffff.ffff.ffff           ffff.ffff.ffff
  3     0100.0000.0000           0100.0000.0000
VLAN filtering table:
  Number of VLANs configured on this interface = 0
  Table entries: Total = 2048, Used = 2, Available = 2046
  Index  VLAN identifier  Enabled  Tunnel
  -----  ---------------  -------  ------
  1           0             No      No
  2           0             Yes     No
Platform details:
  PXF tif number: 0x10
```

The following is sample output from the **showcontrollersgigabitethernet** command for the first fiber interface (port 0) in a 2-Port 10/100/1000 Gigabit Ethernet SPA located in the bottom subslot (1) of the MSC that is installed in slot 4 on a Cisco 7304 router:

```
Router# show controllers gigabitethernet 4/1/0
Interface GigabitEthernet4/1/0
  Hardware is SPA-2GE-7304
  Connection mode is auto-negotiation
  Interface state is up, link is up
  Configuration is Auto Speed, Auto Duplex
  Selected media-type is GBIC, GBIC type is 1000BaseSX
  SFP is present, LOS: no, Tx fault: no, Security check status: Pass
  Promiscuous mode is off, VLAN filtering is enabled
  MDI configuration is automatic crossover, status is MDI
  Auto-negotiation configuration and status:
    Auto-negotiation is enabled and is completed
    Speed/duplex is resolved to 1000 Mbps, full duplex
    Advertised capabilities: 1000BaseX/FD Pause capable (Asymmetric)
    Partner capabilities: 1000BaseX/FD Pause capable(Asymmetric)
MAC counters:
  Input: packets = 213, bytes = 21972
         FIFO full/reset removed = 0, error drop = 0
  Output: packets = 216, bytes = 22932
          FIFO full/reset removed = 0, error drop = 0
  Total pause frames: transmitted = 0, received = 0
FPGA counters:
  Input: Total (good & bad) packets: 213, TCAM drops: 183
         Satisfy (host-backpressure) drops: 0, CRC drops: 0
         PL3 RERRs: 0
  Output: EOP (SPI4) errors: 0
SPA carrier card counters:
  Input: packets = 30, bytes = 10140, drops = 0
  Output: packets = 216, bytes = 22068, drops = 0
  Egress flow control status: XON
  Per bay counters:
  General errors: input = 0, output = 0
  SPI4 errors: ingress dip4 = 0, egress dip2 = 0
MAC destination address filtering table:
  Table entries: Total = 1024, Used = 4, Available = 1020
  Index MAC destination address       Mask
  ----- -----------------------  --------------
  1     0007.0ed3.ba88           ffff.ffff.ffff
  2     ffff.ffff.ffff           ffff.ffff.ffff
  3     0100.0000.0000           0100.0000.0000
  4     0100.0ccc.cccc           ffff.ffff.ffff
VLAN filtering table:
  Number of VLANs configured on this interface = 0
  Table entries: Total = 2048, Used = 2, Available = 2046
  Index  VLAN identifier  Enabled  Tunnel
  -----  ---------------  -------  ------
  1          0              No      No
  2          0              Yes     No
Platform details:
  PXF tif number: 0x14
```

This table describes the fields shown in the interface configuration section of the display. This section is useful for verifying the status of autonegotiation and configured parameters on the link, and the amount of traffic being handled by the interface.

Table 61: show controllers Command Field Descriptions--Interface Section

Field	Description
Interface	Name of the interface.
Hardware	Type of hardware.

Field	Description
Connection mode	Indicator of autonegotiation used to establish the connection.
Link	State of the link.
Configuration	Configuration of the speed and duplex operation on the interface.
Selected media-type	Interface port media type: RJ45 or Gigabit Interface Converter (GBIC).
GBIC type is	GBIC interface type: 1000BaseSX, 1000BaseLX, or 1000BaseZX
SFP is	Indicates presence of an SFP optical transceiver.
LOS	Indicates whether or not the SFP detects a loss of signal (LOS).
Tx fault	Indicates whether or not the SFP detects a transmission fault.
Security check status	Indicates whether or not the SFP passes the security check. The SPA enables a security check by default to verify whether a Cisco-approved SFP is inserted. If the SFP is not a Cisco-approved device, the link is brought down.
Promiscuous mode	State of promiscuous mode (on or off). When promiscuous mode is on, the SPA disables MAC destination address and VLAN filtering. When promiscuous mode is off, the SPA enables MAC destination address and VLAN filtering.
VLAN filtering	Status of ternary content addressable memory (TCAM) filtering of VLANs (enabled or disabled). By default, the SPA always enables VLAN filtering. The SPA disables VLAN filtering if the TCAM table is full, or if the SPA is operating in promiscuous mode. **Note** VLAN filtering is not enabled or disabled using any command-line interface (CLI) command.
MDI crossover status	State of the media dependent interface (MDI) for the PHY device on the specified interface. The possible values are MDI for straight-through cables or media dependent interface crossover (MDI-X) for crossover cables.
Auto-negotiation	State of autonegotiation (enabled or disabled) on the interface and its current status.
Speed/duplex is resolved to	Results of autonegotiated parameter values (speed and duplex) currently being used on the link.
Advertised capabilities	List of the possible combinations of speed and duplex modes (in *speed*/*duplex* format) and flow control that the local interface has advertised it supports to the remote device: • For speed--10M is 10 Mbps, 100M is 100 Mbps, and 1000M is 1000 Mbps. • For duplex--HD is half duplex, and FD is full duplex. • For flow control--“Pause capable (Asymmetric)” means that the SPA advertises support of the PAUSE flow control bit and the ASM_DIR (asymmetric) flow control bit.

Field	Description
Partner capabilities	List of the possible combinations of speed and duplex modes (in *speed*/*duplex* format) and flow control that the remote device has advertised it supports to the local interface: • For speed--10M is 10 Mbps, 100M is 100 Mbps, and 1000M is 1000 Mbps. • For duplex--HD is half duplex, and FD is full duplex. • For flow control--"Pause capable" means that the remote device supports implementation of the PAUSE flow control bit; "Pause capable (Asymmetric)" means that the remote device supports implementation of the PAUSE flow control bit and the ASM_DIR (asymmetric) flow control bit.

This table describes the fields shown in the MAC counters section of the display. This section is useful for verifying the status of packets processed by the MAC device for the interface. This information is useful for Cisco Systems technical support personnel.

Table 62: show controllers Command Field Descriptions--MAC Counters Section

Field	Description
Input: packets, bytes	Total number of packets and bytes received by the MAC device for the interface since it was activated or cleared. You can clear these counters using the **clearcounters** privileged EXEC command.
Input: FIFO full/reset removed	Total number of packets removed by the MAC device due to a first-in, first-out (FIFO) overflow condition in the input buffer for the interface.
Input: error drop	Total number of input packets with errors that are dropped by the MAC device for the interface.
Output: packets, bytes	Total number of packets and bytes transmitted by the MAC device for the interface since it was activated or cleared. You can clear these counters using the **clearcounters** privileged EXEC command.
Output: FIFO full/reset removed	Total number of packets removed by the MAC device due to a first-in, first-out (FIFO) overflow condition in the output buffer for the interface.
Output: error drop	Total number of output packets with errors that are dropped by the MAC device for the interface.
SPI3: disabled port drop	Total number of packets dropped by the MAC device at the System Packet Interface Level 3 (SPI3) path between the MAC device and FPGA device due to a disabled port condition.
SPI3: sync error drop	Total number of packets dropped by the MAC device at the SPI3 path between the MAC device and FPGA device due to a sync error (synchronization bits altered) condition.

Field	Description
SPI3: short packet drop	Total number of packets dropped by the MAC device at the SPI3 path between the MAC device and FPGA device due to a short packet (packet length is less than 64 bytes) condition.
SPI3: parity error drop	Total number of packets dropped by the MAC device at the path between the MAC device and FPGA device due to a parity error (parity bit is altered during data transmission) condition.
Total pause frames	Total number of Ethernet 802.3x pause frames transmitted and received by the MAC device for flow control on the interface.

This table describes the fields shown in the FPGA counters section of the display. This section is useful for verifying the status of packets processed by the FPGA device for the interface. This information is useful for Cisco Systems technical support personnel.

Table 63: show controllers Command Field Descriptions--FPGA Counters Section

Field	Description
Input: Total (good & bad) packets	Total number of packets received by the FPGA device in the ingress direction for the interface.
Input: TCAM drops	Total number of packets dropped by the FPGA device in the ingress direction for the interface due to a ternary content addressable memory (TCAM) lookup failure. This counter increments when the interface receives a frame with a destination MAC address or VLAN identifier that is not present in the TCAM table.
Input: Satisfy (host-backpressure) drops	Total number of packets dropped by the FPGA device in the ingress direction for the interface due to back-pressure from the MSC.
Input: CRC drops	Total number of packets dropped by the FPGA device in the ingress direction for the interface due to cyclic redundancy check (CRC) errors.
Input: PL3 RERRs	Total number of packets with errors received for the interface by the FPGA device in the ingress direction over the SPI3 (PL3) path from the MAC device to the FPGA device.
Output: EOP (SPI4) errors	Total number of packets with end-of-packet (EOP) errors received by the FPGA device in the egress direction for the interface over the System Packet Interface Level 4 (SPI4) path from the MSC to the FPGA device.

The following table describes the fields shown in the SPA carrier card counters section of the display. This section is useful for verifying the status of packets processed by the MSC for the interface. This information is useful for Cisco Systems technical support personnel.

Table 64: show controllers Command Field Descriptions--SPA Carrier Card Counters Section

Field	Description
Input: packets, bytes, drops	Total number of packets, bytes, and packet drops that have occurred on the SPI4 path from the FPGA device to the MSC.
Output: packets, bytes, drops	Total number of packets, bytes, and packet drops that have occurred on the SPI4 path from the MSC to the FPGA device.
Egress flow control status	Status of flow control between the MSC and the Route Processor (RP). The possible values are: • XON--A control frame has been sent by the MSC to the RP to indicate that the MSC is ready to accept data. • XOFF--A control frame has been sent by the MSC to the RP to indicate congestion on the MSC. The MSC cannot accept any more data from the RP during this condition.
General errors	Total number of errors (such as parity) on the MSC in the ingress and egress direction.
SPI4 errors: ingress dip4	Total number of 4-bit Diagonal Interleaved Parity (DIP4) errors in the ingress direction on the SPI4 path from the FPGA device to the MSC. DIP4 is a parity algorithm where a 4-bit odd parity is computed diagonally over control and data words.
SPI4 errors: egress dip2	Total number of 2-bit Diagonal Interleaved Parity (DIP2) errors in the egress direction on the SPI4 path from the FPGA device to the MSC. DIP2 is a parity algorithm where a 2-bit odd parity is computed diagonally over status words.

The following table describes the fields shown in the SPA error counters section of the display. This section appears only when one of the SPI4 transmit or receive errors occurs on the interface. This information is useful for Cisco Systems technical support personnel.

Note None of the SPA SPI4 error counters appear in **showcontrollersgigabitethernet** command output until at least one of those types of SPI4 errors occurs.

All of the errors in the SPA error counters section are subject to the SPA automatic recovery process when certain thresholds are reached. For more information about this process on the Cisco 7304 router, refer to the “Understanding SPA Automatic Recovery” section of the *Cisco 7304 Router Modular Services Card and Shared Port Adapter Software Configuration Guide* .

Table 65: show controllers Command Field Descriptions--SPA Error Counters Section

Field	Description
SPI4 TX out of frame error = (*hh:mm:ss* ago)	Number of SPI4 out of frame errors (events) detected in the transmit direction (toward the network), from the MSC to the SPA FPGA device. The time stamp indicates how long ago (in hours:minutes:seconds) from the current system time, that the last error was detected. This error indicates a loss of synchronization between the synchronization block and the data received on the SPI4 path. When synchronization is reacquired, the error no longer occurs.
SPI4 TX Train valid error = (*hh:mm:ss* ago)	Number of times that a low-level synchronization problem was detected in the transmit direction (toward the network), from the MSC to the SPA FPGA device. The time stamp indicates how long ago (in hours:minutes:seconds) from the current system time, that the last error was detected.
SPI4 TX DIP4 error = (*hh:mm:ss* ago)	Number of 4-bit Diagonal Interleaved Parity (DIP4) errors in the transmit direction (toward the network), from the MSC to the SPA FPGAdevice. The time stamp indicates how long ago (in hours:minutes:seconds) from the current system time, that the last error was detected. DIP4 is a parity algorithm where a 4-bit odd parity is computed diagonally over control and data words.
SPI4 RX out of frame error = (*hh:mm:ss* ago)	Number of SPI4 out of frame errors (events) detected in the receive direction (from the network), from the SPA FPGA device to theMSC. The time stamp indicates how long ago (in hours:minutes:seconds) from the current system time, that the last error was detected. This error indicates a loss of synchronization between the synchronization block and the data received on the SPI4 path. When synchronization is reacquired, the error no longer occurs.
SPI4 RX DIP2 error = (*hh:mm:ss* ago)	Number of 2-bit Diagonal Interleaved Parity (DIP2) errors in the receive direction (from the network), from theSPA FPGA device to the MSC. The time stamp indicates how long ago (in hours:minutes:seconds) from the current system time, that the last error was detected. DIP2 is a parity algorithm where a 2-bit odd parity is computed diagonally over status words.

The following table describes the fields shown in the MAC destination address filtering table section of the display. This section is useful for verifying the multicast destination addresses that are in the TCAM table and permitted by the interface. This information is useful for Cisco Systems technical support personnel.

Table 66: show controllers Command Field Descriptions--MAC Destination Address Filtering Table Section

Field	Description
Table entries: Total, Used	Total number of MAC destination address entries possible in the TCAM table for the interface, and the number of table entries currently used by the interface. The 2-Port 10/100/1000 Gigabit Ethernet SPA supports a 512-entry MAC filtering table for each supported interface (1024 entries total on the card).
Index	Table entry identifier.
MAC destination address	MAC destination address (multicast) permitted by the interface and used in the TCAM lookup table for packet filtering. The multicast MAC entries typically come from routing protocols [such as Open Shortest Path First (OSPF) and Enhanced IGRP (EIGRP)], and other protocols including the Hot Standby Router Protocol (HSRP). When the router reloads, three addresses appear by default in the MAC filtering table: the unicast address of the local interface, the Ethernet broadcast address, and the Ethernet multicast address.
Mask	Mask for the corresponding destination address. The SPA uses the bits that are set in the mask to look up the address in the TCAM table.

The following table describes the fields shown in the VLAN filtering table section of the display. This section is useful for verifying the VLANs that are in the TCAM table and are permitted by the interface. This information is useful for Cisco Systems technical support personnel.

Table 67: show controllers Command Field Descriptions--VLAN Filtering Table Section

Field	Description
Number of VLANs configured on this interface	Number of VLANs that are configured on the interface. If the number of VLANs configured on the interface is 1022 or less, then the VLAN filtering table also shows an index entry for every VLAN ID. The number of VLANs configured on the interface can be 0, while the number of used table entries reports 2, because the SPA always uses two entries to provide valid matching criteria for promiscuous mode and non-VLAN packets.
Table entries: Total, Used, Available	Total number of VLAN entries possible in the TCAM filtering table for the interface, the number of table entries currently used by the interface (two are always in use by default), and the number of table entries that remain available. The 2-Port 10/100/1000 Gigabit Ethernet SPA supports a 1024-entry VLAN filtering table for each supported interface (2048 entries total on the card).
Index	Table entry identifier.
VLAN identifier	Number of the VLAN. Two VLAN ID 0 entries always appear in the table and represent the local interface port for handling of promiscuous mode and non-VLAN packets. Other VLAN entries appear in this table when VLANs are configured on the interface.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Enabled</td><td>Status of the VLAN ID for TCAM filtering, with the following possible values:
• No--The entry is disabled for filtering.
• Yes--The entry is enabled for filtering.

The TCAM filter uses the “first-match” rule to filter packets that the SPA receives against entries in the table. The matching assessment begins at the top of the table with the VLAN ID 0 entries.

Note The SPA always supports two VLAN ID 0 entries. The first VLAN ID 0 entry of the TCAM table is used for promiscuous mode. It has a value of “No,” meaning it is disabled, whenever promiscuous mode is disabled for the interface. The second VLAN ID 0 entry is used for filtering of non-VLAN packets.</td></tr>
<tr><td>Tunnel</td><td>Status of tunneling for the interface, with the following possible values:
• No--Tunneling is disabled and theSPA performs MAC destination address filtering.
• Yes--Tunneling is enabled and the SPA does not perform MAC destination address filtering.

Note If promiscuous mode is enabled, then the first VLAN ID 0 entry shows tunnel = Yes. All other VLAN ID entries show tunnel = No.</td></tr>
</table>

The following table describes the fields shown in the platform details section of the display.

Table 68: show controllers Command Field Descriptions--Platform Details Section

Field	Description
PXF tif number	Number of the interface (in hexadecimal format) used for PXF on the network services engine (NSE) or by the Hyper Transport (HT) FPGA device on the network processing engine (NPE).

Related Commands

Command	Description
show interfaces gigabitethernet	Displays software and hardware information about a Gigabit Ethernet interface.

show controllers integrated-service-engine

To show the Cisco wireless LAN controller network module (WLCM) on the router, use the **showcontrollersintegrated-service-engine** command in privileged EXEC mode.

show controllers integrated-service-engine slot / unit

Syntax Description

slot/unit	Specifies the router slot and unit numbers for the WLCM.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(15)T	This command was introduced.

Examples

The following example shows how to display interface information for the WLCM:

```
Router# show controllers integrated-service-engines
 1/0
Interface integrated-service-engine 1/0
Hardware is Intel 82559 FastEthernet
IDB: 67796B08, FASTSEND: 60E073CC, MCI_INDEX: 0

INSTANCE=0x67797BE8
  Rx Ring entries = 64
  Rx Shadow = 0x67797ED0
  Rx Ring = 0x2DCC1840
  Rx Ring Head = 5
  Rx Ring Last = 4
  Rx Buffer Descr = 0x2DCC3040
  Rx Buffer Descr Head = 5
  Rx Buffer Descr Last = 4

(cont...)
Receive All Multicasts = enabled
Receive Promiscuous = disabled
Loopback Mode = disabled


Module Reset Statistics:
  CLI reset count = 0
  CLI reload count = 0
  Registration request timeout reset count = 0
  Error recovery timeout reset count = 0
  Module registration count = 1
```

show controllers ism

To display controller information for the internal service module interface, use the **showcontrollersism** command in user EXEC or privileged EXEC mode.

show controllers ism *slot/port*

Syntax Description

slot	Router slot in which the service module is installed. For internal service modules, always use 0.
/ *port*	Port number of the module interface. Always use 0. The slash mark (/) is required.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

The output from this command is generally useful for diagnostic tasks performed by technical support only. You can, however, use the displayed hardware statistics to obtain the receive and transmit packet statistics that are collected by the hardware controller during packet processing.

Examples

The following example shows how to display information for the ISM installed in the router:

```
Router# show controllers ism 0/0
Interface ISM0/0
Hardware is PSE2
HWIDB: 0x01395BF0 INSTANCE: 0x11E75280, FASTSEND: 0x040D6C44
Init flags: 0x23

FPGA registers
----------------
  Base address:   0xE2000000    Revision:       0x09030416
  FPGA type:      0x72676D69    FPGA_error_val: 0x00000000
  Cfg MSI mask:   0x00000008    Rx_buffer_size: 0x00000600

Frame statistics: (polling enabled)
-----------------------------------
  tx_frame_cnt: 677                     rx_frame_cnt: 333
  tx_byte_cnt: 104953                   rx_byte_cnt: 35076
  tx_pause_frame_cnt: 0                 rx_pause_frame_cnt: 0
  rx_unicast_filtered_cnt: 0            rx_multicast_filtered_cnt: 8
  rx_undersize_pkts: 0                  rx_oversize_pkts: 0
  tx_64_byte_pkts: 435                  rx_64_byte_pkts: 217
  tx_65_to_127_byte_pkts: 17            rx_65_to_127_byte_pkts: 8
  tx_128_to_255_byte_pkts: 4            rx_128_to_255_byte_pkts: 108
  tx_256_to_511_byte_pkts: 221          rx_256_to_511_byte_pkts: 0
  tx_512_to_1023_byte_pkts: 0           rx_512_to_1023_byte_pkts: 0
  tx_1024_to_1518_byte_pkts: 0          rx_1024_to_1518_byte_pkts: 0
  rx_congestion_drop_cnt: 0             rx_mtusize_drop_cnt: 0
  rx_bad_cnt: 0

Interrupt statistics
--------------------
  ge_tx_interrupt: 569                  ge_rx_interrupt: 326
```

```
  txbd_seq_err: 0                       txbd_done_err: 0
  rxbd_done_err: 0                      isl_inner_crc_err: 0
  pcie_busmstr_dsbld_err: 0             pcie_tgt_abort_err: 0
  pcie_mst_abort_err: 0                 spi_done_event: 0
  rx_empty_pak: 0                       rx_sw_usage_err: 0
  ing_buf_adrs_err: 0                   pcie_null_ptr_err: 0
  uart_tx_intr: 58                      uart_rx_intr: 9036
  uart_break_detected: 0                uart_framing_err: 0
  uart_bad_egr_adrs: 0                  uart_egr_overflow: 0
  i2c_errs: misc/nack/tmo: 0/0/0

TX ring
-------
  Tx Ring txr_head/txr_tail:  167/167
  Tx Shadow txs_head/txs_tail/txs_free: 167/167/256
  Tx Ring(txr): 0x3CF84800 Tx Shadow (malloc): 0x11E75500
  Tx Limited: 0 Tx Count: 0 hold_pak 0x00000000

RX rings
--------
  size: 256      max_spin_size 32       head: 70
  Rx Ring(rxr):   0x3CF84000  rxr_malloc: 0x3CF84000
  Rx Shadow(rxs): 0x13969F4   rxs_malloc: 0x13969F4

Software MAC Address Filter (hash:length/addr/mask/hits)
--------------------------------------------------------
   000:  0  ffff.ffff.ffff  0000.0000.0000         2
   039:  0  001e.4a97.646d  0000.0000.0000         0
   192:  0  0180.c200.0002  0000.0000.0000         0
   192:  1  0100.0ccc.cccc  0000.0000.0000       106
   197:  0  0180.c200.0007  0000.0000.0000         0

   Software filtered frames: 0
   Unicast overflow mode:   0
   Multicast overflow mode: 1
   Promiscuous mode:        0

  HW MAC Address Filter
  ---------------------
   Unicast Addr0: 001E.4A97.646D
   Unicast Addr1: 0000.0000.0100
   Unicast Addr2: 0000.0000.0100
   Unicast Addr3: 0000.0000.0100
   Unicast Addr4: 0000.0000.0100
   Unicast HW Filter Count   : 1

   Multicast Hash b63_32: 0x2000001
   Multicast Hash b32_00: 0x00
   HW unicast filter enabled: Yes
   HW multicast filter enabled: Yes

FPGA upgrade info
-----------------
  Golden area fpga version:  00000000
  Upgrade area fpga version: 09030416
  IOS bundled fpga version:  09030416
```

The table below describes the significant fields shown in the display.

Table 69: show controllers analysis-module Field Descriptions

Field	Description
Hardware	Description of the chip being used.
IDB, FASTSEND	Address in router memory of the Interface Descriptor Block (IDB) and the fastsend routine.
INSTANCE	Device-specific data stored in router memory that lists the memory locations and current indexes of receive (Rx) and transmit (Tx) rings in router I/O memory.
CONTROL AND STATUS REGISTERS (CSR)	Control and status registers that are physically located on the chip itself and that are accessed by the CPU over the Peripheral Component Interconnect (PCI) bus.
PHY REGISTERS	Contents of the PHY registers. PHY is a device that interfaces the physical Ethernet line and that is located between the chip and the physical line.
HARDWARE STATISTICS	Receive (Rx) and transmit (Tx) traffic statistics collected by the chip.
INTERRUPT STATISTICS	Transmit (Tx), Receive (Rx), control, software, and flow control interrupt statistics collected by the chip.

Related Commands

Command	Description
service-module ism status	Displays hardware and software status information about the ISM.
show interfaces ism	Displays status, traffic data, and configuration information about the ISM interface.

show controllers j1

To display statistics about the J1 link, use the **showcontrollersj1**command in privileged EXEC mode.

show controllers j1 *slot/port*

Syntax Description

slot / port	Backplane slot and port number on the controller.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(8)T	The command was introduced on the J1 controller for the Cisco 2600 and Cisco 3600 series.

Examples

The following is sample output from the **showcontrollersj1**command on the Cisco 3660:

```
Router# show controllers j1 3/0
J1 3/0 is up.
  Applique type is Channelized J1 - TTC2M
  No alarms detected.
Version info Firmware: 20010530, FPGA: 1
  Framing is J1-TTC2M MF, Line Code is CMI, Clock Source is Line.
  Data in current interval (344 seconds elapsed):
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
  Total Data (last 24 hours)
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins,
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
```

The table below describes the fields shown in the display.

Table 70: show controllers j1 Field Descriptions

Field	Description
j1 3/0 is up.	The J1 controller 3 in slot 0 is operating. The controller's state can be up, down, or administratively down.
Applique type	The applique type is shown and is always Channelized.

Field	Description
No alarms detected	Any alarms detected by the controller are displayed here. Possible alarms are as follows: • Transmitter is sending remote alarm. • Transmitter is sending AIS. • Receiver has loss of signal. • Receiver is getting AIS. • Receiver has loss of frame. • Receiver has remote alarm. • Receiver has no alarms.
Version	Indicates date of compilation.
Framing is	Shows the current framing type which is always J1-TTC2M MF.
Linecode is	Shows the current line encoding type which is always coded mark inversion (CMI).
Clock Source	Shows the current clock source type.
Data in current interval (344 seconds elapsed)	Shows the current accumulation period, which rolls into the 24-hour accumulation every 15 minutes. Accumulation period is from 1 to 900 seconds. The oldest 15-minute period falls off the back of the 24-hour accumulation buffer.
Slip Secs	Indicates the replication or deletion of the payload bits of a DS1 frame. A slip might be performed when there is a difference between the timing of a synchronous receiving terminal and the received signal.
Fr Loss Secs	Indicates the number of seconds an Out of Frame (OOF) error is detected.
Line Err Secs	Line errored seconds (LES) is a second in which one or more line code violation errors are detected.
Degraded Mins	A degraded minute is one in which the estimated error rate exceeds 1E-6 but does not exceed 1E-3.
Errored Secs	An errored second is a second in which one of the following are detected: • One or more path code violations. • One or more out of rame defects. • One or more controlled slip events. • A detected alarm indication signal (AIS) defect.

Field	Description
Bursty Err Secs	A second with fewer than 320 and more than 1 path coding violation error, no severely errored frame defects, and no detected incoming AIS defects. Controlled slips are not included in this parameter.
Severely Err Secs	A severely err sec is a second with one of the following errors: 320 or more path code violation errors; one or more out of frame defects; a detected AIS defect.
Unavail Secs	A count of the total number of seconds where the controller did not get a clock.

show controllers lex

To show hardware and software information about the LAN Extender chassis, use the **showcontrollerslex** command in EXEC mode.

show controllers lex [*number*]

Cisco 7500 Series
show controllers lex [*slot*/*port*]

Syntax Description

number	(Optional) Number of the LAN Extender interface about which to display information.
slot	(Optional) Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information.
port	(Optional) Number of the port being configured. Refer to the appropriate hardware manual for slot and port information.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(15)T	This command is no longer supported in Cisco IOS Mainline or Technology-based releases. It may conintue to appear in Cisco IOS 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **showcontrollerslex** command to display information about the hardware revision level, software version number, Flash memory size, serial number, and other information related to the configuration of the LAN Extender.

Examples

The following is a sample output from the **showcontrollerslex** command:

```
Router# show controllers lex 0
Lex0:
FLEX Hardware revision 1
FLEX Software version 255.0
128K bytes of flash memory
Serial number is 123456789
Station address is 0000.4060.1100
```

The following is a sample output from the **showcontrollerslex** command when the LAN Extender interface is not bound to a serial interface:

```
Router#
```

```
show controllers lex 1
Lex1 is not bound to a serial interface
```

The table below describes the fields shown in the preceding output.

Table 71: show controllers lex Field Descriptions

Field	Description
Lex0:	Number of the LAN Extender interface.
FLEX Hardware revision	Revision number of the Cisco 1000 series LAN Extender chassis.
FLEX Software version	Revision number of the software running on the LAN Extender chassis.
128K bytes of Flash memory	Amount of Flash memory in the LAN Extender.
Serial number	Serial number of the LAN Extender chassis.
Station address	MAC address of the LAN Extender chassis.

show controllers mci

To display all information under the Multiport Communications Interface (MCI) card or the Serial Communications Interface (SCI) card, use the **showcontrollersmci** command in privileged EXEC mode.

show controllers mci

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command displays information that the system uses for bridging and routing that is specific to the interface hardware. The information displayed is generally useful for diagnostic tasks performed by technical support personnel.

The interface type is queried only at startup. If the hardware changes *subsequent* to initial startup, the wrong type is reported. This has *no* adverse effect on the operation of the software. For instance, if a DCE cable is connected to a dual-mode V.35 applique after the unit has been booted, the display presented for the **showinterfaces** command incorrectly reports attachment to a DTE device although the software recognizes the DCE interface and behaves accordingly.

Examples

The following is sample output from the **showcontrollersmci** command:

```
Router# show controllers mci
MCI 0, controller type 1.1, microcode version 1.8
    128 Kbytes of main memory, 4 Kbytes cache memory
22 system TX buffers, largest buffer size 1520
    Restarts: 0 line down, 0 hung output, 0 controller error
Interface 0 is Ethernet0, station address 0000.0c00.d4a6
    15 total RX buffers, 11 buffer TX queue limit, buffer size 1520
    Transmitter delay is 0 microseconds
Interface 1 is Serial0, electrical interface is V.35 DTE
    15 total RX buffers, 11 buffer TX queue limit, buffer size 1520
    Transmitter delay is 0 microseconds
    High speed synchronous serial interface
Interface 2 is Ethernet1, station address aa00.0400.3be4
    15 total RX buffers, 11 buffer TX queue limit, buffer size 1520
    Transmitter delay is 0 microseconds
Interface 3 is Serial1, electrical interface is V.35 DCE
    15 total RX buffers, 11 buffer TX queue limit, buffer size 1520
    Transmitter delay is 0 microseconds
    High speed synchronous serial interface
```

The table below describes significant fields shown in the display.

Table 72: show controllers mci Field Descriptions

Field	Description
MCI 0	Card type and unit number (varies depending on card).
controller type 1.1	Version number of the card.
microcode version 1.8	Version number of the card's internal software (in ROM).
128 Kbytes of main memory	Amount of main memory on the card.
4 Kbytes cache memory	Amount of cache memory on the card.
22 system TX buffers	Number of buffers that hold packets to be transmitted.
largest buffer size 1520	Largest size of these buffers (in bytes).
Restarts • 0 line down • 0 hung output • 0 controller error	Count of restarts for the following conditions: • Communication line down • Output unable to transmit • Internal error
Interface 0 is Ethernet0	Names of interfaces, by number.
electrical interface is V.35 DTE	Line interface type for serial connections.
15 total RX buffers	Number of buffers for received packets.
11 buffer TX queue limit	Maximum number of buffers in transmit queue.
Transmitter delay is 0 microseconds	Delay between outgoing frames.
Station address 0000.0c00.d4a6	Hardware address of the interface.

Related Commands

Command	Description
tx-queue-limit	Controls the number of transmit buffers available to a specified interface on the MCI and SCI cards.

show controllers pcbus

To display all information about the bus interface, use the **showcontrollerspcbus** command in privileged EXEC mode.

show controllers pcbus

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is valid on LanOptics Branchcard or Stacknet 2000 products only.

Examples

The following is sample output from the **showcontrollerspcbus** command:

```
Router# show controllers pcbus
PCbus unit 0, Name = PCbus0  Hardware is ISA PCbus shared RAM
IDB at 0x3719B0, Interface driver data structure at 0x3735F8
Control/status register at 0x2110008, Shared memory at 0xC000000
Shared memory is initialized

Shared memory interface control block :
Magic no = 0x41435A56 (valid) Version = 1.0
Shared memory size = 64K bytes, Interface is NOT shutdown
Interface state is up, line protocol is up

Tx buffer : (control block at 0xC000010)
Start offset = 0x30, Size = 0x7FE8, Overflows = 1
GET_ptr = 0x4F6C, PUT_ptr = 0x4F6C, WRAP_ptr = 0x3BB0

Rx buffer : (control block at 0xC000020)
Start offset = 0x8018, Size 0x7FE8, Overflows = 22250698
GET_ptr = 0x60, PUT_ptr = 0x60, WRAP_ptr = 0x7FD0

Interrupts received = 567
```

show controllers pos

To display information about the Packet over SONET (POS) controllers, use the **showcontrollerspos** command in privileged EXEC mode.

Cisco 7500 Series Routers
show controllers pos [*slot*/*port-adapter*/*port*] [{**details** | **pm** [*time-interval*]}]

Cisco 12000 Series Routers
show controllers pos [*slot*/*port*] [{**details** | **pm** [*time-interval*]}]

POS Shared Port Adapters
show controllers pos [*slot*/*subslot*/*port* [/*sub_int*]] [{**alarm** | **details** | **pm** [*time-interval*]}]

Syntax Description

slot / *port-adapter* / *port*	**(Optional) Cisco 7500 Series Routers** Number of the chassis slot that contains the POS interface (for example, 2/0/0), where: • *slot* --Chassis slot number. • / *port-adapter*-- Port adapter number. • / *port*-- Port or interface number. Refer to the appropriate hardware manual for slot and port information, and port adapter compatibility.
slot / *port*	**(Optional) Cisco 12000 Series Routers** Number of the chassis slot that contains the POS interface (for example, 4/0), where: • *slot* --Chassis slot number. • / *port*-- Port or interface number. Refer to the appropriate hardware manual for slot and port information.

slot / *subslot* / *port* / *sub_int*	**(Optional) POS Shared Port Adapters** Number of the chassis slot that contains the POS interface (for example 4/3/0), where: • *slot* --Chassis slot number. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide. • / *subslot*-- Secondary slot number on a SPA interface processor (SIP) where a SPA is installed. Refer to the platform-specific SPA hardware installation guide and the corresponding "Specifying the Interface Address on a SPA" topic in the platform-specific SPA software configuration guide for subslot information. • / *port* --Port or interface number. For SPAs, refer to the corresponding "Specifying the Interface Address on a SPA" topics in the platform-specific SPA software configuration guide. • / *sub_int* -- (Optional) Subinterface number.
alarm	(Optional) Displays SONET/SDH alarm event counters.
details	(Optional) In addition to the normal information displayed by the **showcontrollerspos** command, the **details** keyword provides a hexadecimal and ASCII "dump" of the path trace buffer.
pm	(Optional) Displays SONET performance monitoring statistics accumulated for a 24-hour period in 15-minute intervals.
time-interval	(Optional) Number of the SONET MIB 15-minute time interval in the range from 1 to 96. If the *time-interval*argument is not specified, the performance monitoring statistics for the current time interval are displayed.

Command Default

If you do not specify any slot addressing, information for all installed POS interfaces is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1CC	This command was introduced.
12.2S	This command was integrated into Cisco IOS Release 12.2S.
12.2(25)S3	This command was integrated into Cisco IOS Release 12.2(25)S3 to support SPAs on the Cisco 7304 router. The command was modified to support a new addressing format for SPAs on the Cisco 7304 router.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE to support SPAs on the Cisco 7600 series routers and Catalyst 6500 series switches.

Release	Modification
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S to support SPAs on the Cisco 12000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **showcontrollerspos** command with the **pm** keyword displays SONET performance monitoring statistics accumulated at 15-minute intervals, and these statistics can be queried using Simple Network Management Protocol (SNMP) tools. The performance monitoring statistics are collected according to the RFC 1595 specification.

The information that this command displays is generally useful only for diagnostic tasks performed by Cisco Systems technical support personnel.

Examples

Example of the show controllers pos Command on the Cisco 7500 Series Router

The following is sample output from the **showcontrollerspos** command on a Cisco 7500 series router:

```
Router# show controllers pos
POS2/0/0
SECTION
  LOF = 0          LOS = 2335                        BIP(B1) = 77937133
LINE
  AIS = 2335       RDI = 20         FEBE = 3387950089 BIP(B2) = 1622825387
PATH
  AIS = 2340       RDI = 66090      FEBE = 248886263  BIP(B3) = 103862953
  LOP = 246806     NEWPTR = 11428072   PSE = 5067357     NSE = 4645
Active Defects: B2-TCA B3-TCA
Active Alarms:  None
Alarm reporting enabled for: B1-TCA
APS
  COAPS = 12612784   PSBF = 8339
  State: PSBF_state = False
  Rx(K1/K2): 00/CC  Tx(K1/K2): 00/00
  S1S0 = 03, C2 = 96
CLOCK RECOVERY
  RDOOL = 64322060
  State: RDOOL_state = True
PATH TRACE BUFFER: UNSTABLE
  Remote hostname :
  Remote interface:
  Remote IP addr  :
  Remote Rx(K1/K2): ../..  Tx(K1/K2): ../..
BER thresholds:  SF = 10e-3  SD = 10e-8
TCA thresholds:  B1 = 10e-7  B2 = 10e-3  B3 = 10e-6
```

The table below describes the fields shown in this display.

Table 73: show controllers pos Field Descriptions

Field	Description
POS*x/y/z*	Slot number of the POS interface.

Field	Description
LOF	Section loss of frame is detected when a severely error framing (SEF) defect on the incoming SONET signal persist for 3 milliseconds.
LOS	Section loss of signal is detected when an all-zeros pattern on the incoming SONET signal lasts 19 plus or minus 3 microseconds or longer. This defect might also be reported if the received signal level drops below the specified threshold.
BIP(B1)/BIP(B2)/BIP(B3)	Bit interleaved parity (BIP). For B1, the BIP error report is calculated by comparing the BIP-8 code with the BIP-8 code extracted from the B1 byte of the following frame. Differences indicate that section-level bit errors have occurred. For B2, the BIP error report is calculated by comparing the BIP-8/24 code with the BIP-8 code extracted from the B2 byte of the following frame. Differences indicate that line-level bit errors have occurred. For B3, the BIP error report is calculated by comparing the BIP-8 code with the BIP-8 code extracted from the B3 byte of the following frame. Differences indicate that path-level bit errors have occurred.
AIS	Alarm indication signal. A line alarm indication signal is sent by the section terminating equipment (STE) to alert the downstream line terminating equipment (LTE) that a loss of signal (LOS) or loss of frame (LOF) defect has been detected on the incoming SONET section. A path alarm indication signal is sent by the LTE to alert the downstream path terminating equipment (PTE) that it has detected a defect on its incoming line signal.
RDI	Remote defect indication. A line remote defect indication is reported by the downstream LTE when it detects LOF, LOS, or AIS. A path remote defect indication is reported by the downstream PTE when it detects a defect on the incoming signal.
FEBE	Far end block errors. Line FEBE (accumulated from the M0 or M1 byte) is reported when the downstream LTE detects BIP(B2) errors. Path FEBE (accumulated from the G1 byte) is reported when the downstream PTE detects BIP(B3) errors.
LOP	Path loss of pointer is reported as a result of an invalid pointer (H1, H2) or an excess number of new data flag (NDF)-enabled indications.
NEWPTR	Inexact count of the number of times that the SONET framer has validated a new SONET pointer value (H1, H2).

Field	Description
PSE	Inexact count of the number of times that the SONET framer has detected a positive stuff event in the received pointer (H1, H2).
NSE	Inexact count of the number of times that the SONET framer has detected a negative stuff event in the received pointer (H1, H2).
Active Defects	List of all currently active SONET defects.
Active Alarms	List of current alarms as enforced by Sonet Alarm Hierarchy.
Alarm reporting enabled for	List of alarms for which you enabled reporting with the **posreport** interface command.
APS	Automatic protection switching.
COAPS	An inexact count of the number of times that a new APS value has been detected in the K1, K2 bytes.
PSBF	An inexact count of the number of times that a protection switching byte failure has been detected (no three consecutive SONET frames contain identical K1 bytes).
PSBF_state	Protection switching byte failure state.
Rx(K1/K2)/Tx(K1/K2)	Contents of the received and transmitted K1 and K2 bytes.
S1S0	The two S bits received in the last H1 byte.
C2	The value extracted from the SONET path signal label byte (C2).
CLOCK RECOVERY	The SONET clock is recovered using information in the SONET overhead. RDOOL is an inexact count of the number of times that Receive Data Out Of Lock has been detected, which indicates that the clock recovery phased lock loop is unable to lock to the receive stream.
PATH TRACE BUFFER	SONET path trace buffer is used to communicate information regarding the remote host name, interface name and number, and IP address. This is a Cisco-proprietary use of the J1 (path trace) byte.
BER thresholds	List of the bit error rate (BER) thresholds that you configured with the **posthreshold** interface command.
TCA thresholds	List of the threshold crossing alarms (TCAs) that you configured with the**posthreshold** interface command.

Example of the show controllers pos Command on a POS Shared Port Adapter

The following is sample output from the **showcontrollerspos** command on a Cisco 7600 series router for POS interface 4/3/0 (which is the interface for port 0 of the SPA in subslot 3 of the SIP in chassis slot 4):

```
Router# show controllers pos 4/3/0

POS4/3/0
SECTION
  LOF = 0          LOS    = 0                            BIP(B1) = 65535
LINE
  AIS = 0          RDI    = 0          FEBE = 65535      BIP(B2) = 16777215
PATH
  AIS = 0          RDI    = 0          FEBE = 65535      BIP(B3) = 65535
  PLM = 0          UNEQ   = 0          TIM  = 0          TIU     = 0
  LOP = 0          NEWPTR = 3          PSE  = 0          NSE     = 0
Active Defects: None
Active Alarms:  None
Alarm reporting enabled for: SF SLOS SLOF B1-TCA B2-TCA PLOP B3-TCA
Framing: SONET
APS
  COAPS = 1          PSBF = 0
  State: PSBF_state = False
  Rx(K1/K2): 00/00  Tx(K1/K2): 00/00
  Rx Synchronization Status S1 = 00
  S1S0 = 00, C2 = CF
  Remote aps status (none); Reflected local aps status (none)
CLOCK RECOVERY
  RDOOL = 0
  State: RDOOL_state = False
PATH TRACE BUFFER: STABLE
  Remote hostname : woodson
  Remote interface: POS3/0/0
  Remote IP addr  : 0.0.0.0
  Remote Rx(K1/K2): 00/00  Tx(K1/K2): 00/00
BER thresholds:  SF = 10e-3  SD = 10e-6
TCA thresholds:  B1 = 10e-6  B2 = 10e-6  B3 = 10e-6
  Clock source:  internal
```

The table below describes the fields shown in this display.

Example of the show controllers pos alarm Command on the Cisco 7600 Series Router

The following is sample output from the **showcontrollersposalarm** command that displays SONET/SDH alarm event counters on a Cisco 7600 series router:

```
Router# show controllers pos3/2/0 alarm
POS3/2/0
Alarm Event Statistics:
SECTION
  LOF = 0          LOS    = 0          B1-TCA = 0
LINE
  AIS = 0          RDI    = 0          RDOOL  = 0
  SF  = 0          SD     = 0          B2-TCA = 0
PATH
  AIS = 0          RDI    = 0          LOP    = 0          B3-TCA = 0
  PLM = 0          UNEQ   = 0
```

Example of the show controllers pos pm Command on the Cisco 12000 Series Router

The following is sample output from the **showcontrollerspospm** command that displays performance monitoring statistics on a Cisco 12000 series router:

```
Router# show controllers pos 1/0 pm
POS1/0
Medium is SONET
Line coding is RZ, Line type is LONG SM
Data in current interval (516 seconds elapsed)
SECTION ( NO DEFECT )
    515 Errored Secs, 515 Severely Err Secs
    0 Coding Violations, 515 Sev Err Framing Secs
LINE ( NO DEFECT )
    0 Errored Secs, 0 Severely Err Secs
    0 Coding Violations, 0 Unavailable Secs
FAR END LINE
    0 Errored Secs, 0 Severely Err Secs
    0 Coding Violations, 0 Unavailable Secs
PATH ( NO DEFECT )
    0 Errored Secs, 0 Severely Err Secs
    0 Coding Violations, 0 Unavailable Secs
FAR END PATH
    0 Errored Secs, 0 Severely Err Secs
    0 Coding Violations, 0 Unavailable Secs
```

The table below describes the fields shown in the display.

Table 74: show controllers pos pm Field Descriptions

Field	Description
POS*x/y*	Slot number of the POS interface.
Line coding	Shows the current line encoding type, either return to zero (RZ) or nonreturn to zero (NRZ).
Line type	Line type for this interface. Optical line types can be either long range (LONG) or short range (SHORT), and either single mode (SM) or multimode (MM).
Data in current interval	Shows the current accumulation period, which rolls into the 24-hour accumulation every 15 minutes. Accumulation period is from 1 to 900 seconds. The oldest 15-minute period falls off the back of the 24-hour accumulation buffer.
Errored Secs	An errored second is a second in which one of the following is detected: • One or more coding violations. • One or more incoming defects (for example, a severely errored frame [SEF] defect, an LOS defect, an AIS defect, or an LOP defect).
Severely Err Secs	A severely errored second (SES) is a second with one of the following errors: • A certain number of coding violations. The number is dependent on the line rate and the BER. • A certain number of incoming defects.
Coding Violations	Number of coding violations for the current interval. Coding violations are defined as BIP errors that are detected in the incoming signal. The coding violations counter is incremented for each BIP error detected.
Sev Err Framing Secs	Severely errored framing seconds (SEFS) are seconds with one or more SEF defects.

Field	Description
Unavailable Secs	Total number of seconds for which the interface is unavailable. The interface is considered to be unavailable after a series of ten consecutive SESs.

Related Commands

Command	Description
pos report	Permits selected SONET alarms to be logged to the console for a POS interface.
pos threshold	Sets the BER threshold values of specified alarms for a POS interface.

show controllers satellite

To display controller information about the internal router interface that connects to an installed Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT), use the **showcontrollerssatellite** command in user EXEC or privileged EXEC mode.

show controllers satellite *slot/unit*

Syntax Description

slot	Router chassis slot in which the network module is installed.
unit	Interface number. For NM-1VSAT-GILAT network modules, always use 0.

Command Default

No default behavior or values.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The output from this command is generally useful for diagnostic tasks performed by technical support.

The **showcontrollerssatellite** command displays information about initialization block, transmit ring, receive ring, and errors for the Fast Ethernet controller chip in the internal router interface that connects to an installed Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT).

Examples

The following example shows how to display controller information about the internal router interface that connects to an installed NM-1VSAT-GILAT network module:

```
Router# show controllers satellite
 2/0

Interface Satellite2/0
Hardware is Intel 82559 FastEthernet
IDB:640B6584, FASTSEND:60A585E0, MCI_INDEX:0
INSTANCE=0x640B7D84
  Rx Ring entries = 64
  Rx Shadow = 0x640B8054
  Rx Ring = 0x 70FEE80
  Rx Ring Head = 51
  Rx Ring Last = 50
  Rx Buffer Descr = 0x 70FF2C0
  Rx Buffer Descr Head = 51
  Rx Buffer Descr Last = 50
  Rx Shadow (malloc) = 0x640B8054
  Rx Ring (malloc) = 0x 70FEE80
  Rx Buffer Descr (malloc) = 0x 70FF2C0
  Tx Ring entries = 128
  Tx Shadow = 0x640B8184
  Tx Shadow Head = 78
  Tx Shadow Tail = 78
  Tx Shadow Free = 128
  Tx Ring = 0x 70FF700
```

```
  Tx Head = 80
  Tx Last = 79
  Tx Tail = 80
  Tx Count = 0
  Tx Buffer Descr = 0x 7100740
  Tx Buffer Descr Head = 0
  Tx Buffer Descr Tail = 0
  Tx Shadow (malloc) = 0x640B8184
  Tx Ring (malloc) = 0x 70FF700
  Tx Buffer Descr (malloc) = 0x 7100740
CONTROL AND STATUS REGISTERS (CSR)=0x3E000000
  SCB Intr Mask    = 00
  SCB CU/RU Cmd    = 00
  SCB Intr Status  = 00
  SCB CU Status    = 01
  SCB RU Status    = 04
  SCB General Ptr  = 00000000
  PORT             = 00000000
  EEPROM           = 0008
  FLASH            = 0002
  MDI              = 1821780D
  Rx Byte Count    = 00000608
  PMDR             = 80
  FC Cmd           = 00
  FC Threshold     = 03
  Early Rx         = 00
  General Status   = 03
  General Control  = 00
PHY REGISTERS
  Register 0x00:  2000  780D  02A8  0154  0081  0000  0000  0000
  Register 0x08:  0000  0000  0000  0000  0000  0000  0000  0000
  Register 0x10:  0202  0000  0001  0005  0000  0000  0000  0000
  Register 0x18:  0000  0000  8B10  0000  0010  0000  0000  0000
HARDWARE STATISTICS
  Rx good frames:        420979
  Rx CRC:                0
  Rx alignment:          0
  Rx resource:           0
  Rx overrun:            0
  Rx collision detects:  0
  Rx short:              0
  Tx good frames:        653125
  Tx maximum collisions: 0
  Tx late collisions:    0
  Tx underruns:          0
  Tx lost carrier sense: 9
  Tx deferred:           86
  Tx single collisions:  1
  Tx multiple collisions:1
  Tx total collisions:   3
  FC Tx pause:           0
  FC Rx pause:           0
  FC Rx unsupported:     0
INTERRUPT STATISTICS
  CX  = 653136
  FR  = 420979
  CNA = 0
  RNR = 0
  MDI = 0
  SWI = 0
  FCP = 0
Receive All Multicasts = enabled
Receive Promiscuous = disabled
Loopback Mode = disabled
```

The table below describes the significant fields shown in the display.

Table 75: show controllers satellite Field Descriptions

Field	Description
Hardware	Description of the chip being used.
IDB	Address in router memory of the Interface Descriptor Block (IDB).
FASTSEND	Fastsend routine.
INSTANCE	Device-specific data stored in router memory that lists the memory locations and current indices of receive (Rx) and transmit (Tx) rings in router I/O memory.
CONTROL AND STATUS REGISTERS (CSR)	Control and status registers that are physically located on the chip itself and that are accessed by the CPU over the protocol control information (PCI) bus.
PHY REGISTERS	Contents of the physical layer (PHY) registers of the PHY module, which is an internal device that interfaces between the internal physical Ethernet line and the external physical line.
HARDWARE STATISTICS	Receive (Rx) and transmit (Tx) traffic statistics collected by the chip.
INTERRUPT STATISTICS	Receive (Rx), transmit (Tx), control, software, and flow control interrupt statistics collected by the chip.

Related Commands

Command	Description
service-module satellite status	Displays status information related to the hardware and software on the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT), including the initial configuration parameters.
show interfaces satellite	Displays general interface settings and traffic rates for the internal router interface that connects to an installed Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT).

show controllers serial through show hw-module slot proc cpu

show cem circuit

To display information about the circuit state, administrative state, the CEM ID of the circuit, and the interface on which it is configured, use the **show cem circuit** command. If cross connect is configured under the circuit, the command output also includes information about the attachment circuit status.

Syntax Description

Syntax Description

Command Default

There is no default.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
XE 3.18 SP	Support for this command was introduced on Cisco NCS 4200 Series.
XE Everest 16.5.1	This command was integrated into the Cisco NCS 4200 Series and Cisco ASR 900 Series Routers.

Usage Guidelines

The **show cem circuit** command allows you to display information about the circuit state, administrative state, the CEM ID of the circuit, and the interface on which it is configured.

Examples

The following example shows the detailed information about a particular circuit.:

```
Router# show cem circuit 0
CEM0/1/2, ID: 0, Line: UP, Admin: UP, Ckt: ACTIVE
Controller state: up, T1/E1 state: up
Idle Pattern: 0xFF, Idle CAS: 0x8
Dejitter: 5 (In use: 0)
Payload Size: 192
Framing: Unframed
CEM Defects Set
None
Signalling: No CAS
RTP: No RTP
Ingress Pkts: 11060 Dropped: 0
Egress Pkts: 11061 Dropped: 0
CEM Counter Details
Input Errors: 0 Output Errors: 0
Pkts Missing: 0 Pkts Reordered: 0
Misorder Drops: 0 JitterBuf Underrun: 0
Error Sec: 0 Severly Errored Sec: 0
Unavailable Sec: 0 Failure Counts: 0
Pkts Malformed: 0 JitterBuf Overrun: 0
```

show controllers serial

To display serial controller statistics, use the **showcontrollersserial**command in privileged EXEC mode.

Standard Syntax
show controllers serial [*slot*/*port*]

Cisco 7000 Series Routers with the RSP7000 and RSP7000CI and Cisco 7500 Series Routers
show controllers serial [*slot*/*port-adapter*/*port*]

T3/E3 Shared Port Adapters and 2-Port and 4-Port Channelized T3 SPA in Unchannelized Mode
show controllers serial [*slot*/*subslot*/*port*]

Channelized T3 Shared Port Adapters
show controllers serial [*slot*/*subslot*/*port*/*t1-number*]

Syntax Description

slot	(Optional) Chassis slot number. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding “Identifying Slots and Subslots for SIPs and SPAs” topic in the platform-specific SPA software configuration guide.
port-adapter	(Optional) On Cisco 7500 series routers and Cisco 7000 series routers with the RSP7000 and RSP7000CI, the location of the port adapter on a Versatile Interface Processor (VIP). The value can be 0 or 1.
/ *subslot*	(Optional) Secondary slot number on a SIP where a SPA is installed. Refer to the platform-specific SPA hardware installation guide and the corresponding “Specifying the Interface Address on a SPA” topic in the platform-specific SPA software configuration guide for subslot information.
/ *port*	(Optional) Port or interface number. Refer to the appropriate hardware manual for port information. For SPAs, refer to the corresponding “Specifying the Interface Address on a SPA” topics in the platform-specific SPA software configuration guide.
t1-number	(Optional) Logical T1 number in channelized mode. For SPAs, refer to the corresponding “Specifying the Interface Address on a SPA” topics in the platform-specific SPA software configuration guide.

Command Default

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.

Release	Modification
11.1CA	This command was modified to include support for the PA-E3 and PA-T3 port adapters.
12.2S	This command was integrated into Cisco IOS Release 12.2S.
12.2(25)S3	This command was integrated into Cisco IOS Release 12.2(25)S3.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE and introduced a new output for interfaces on the serial SPAs on the Cisco 7600 series routers and Catalyst 6500 series switches.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The output from the **showcontrollersserial**command provides error and alarm information that is useful in troubleshooting line problems.

The information displayed is generally useful for diagnostic tasks performed by Cisco Systems technical support personnel only. For the PA-E3 or PA-T3 port adapters, the **showcontrollersserial** command also displays configuration information such as the framing, clock source, bandwidth limit, whether scrambling is enabled, the national bit, the international bits, and DSU mode configured on the interface. Also displayed are the performance statistics for the current interval and last 15-minute interval and whether any alarms exist.

Examples

Example of the show controllers serial Command on the Cisco 4000 Series Router

The following is sample output from the **showcontrollersserial** command on the Cisco 4000:

```
Router# show controllers serial
MK5 unit 0, NIM slot 1, NIM type code 7, NIM version 1
idb = 0x6150, driver structure at 0x34A878, regaddr = 0x8100300
IB at 0x6045500: mode=0x0108, local_addr=0, remote_addr=0
N1=1524, N2=1, scaler=100, T1=1000, T3=2000, TP=1
buffer size 1524
DTE V.35 serial cable attached
RX ring with 32 entries at 0x45560 : RLEN=5, Rxhead 0
00 pak=0x6044D78  ds=0x6044ED4 status=80 max_size=1524 pak_size=0
01 pak=0x60445F0  ds=0x604474C status=80 max_size=1524 pak_size=0
02 pak=0x6043E68  ds=0x6043FC4 status=80 max_size=1524 pak_size=0
03 pak=0x60436E0  ds=0x604383C status=80 max_size=1524 pak_size=0
04 pak=0x6042F58  ds=0x60430B4 status=80 max_size=1524 pak_size=0
05 pak=0x60427D0  ds=0x604292C status=80 max_size=1524 pak_size=0
06 pak=0x6042048  ds=0x60421A4 status=80 max_size=1524 pak_size=0
07 pak=0x60418C0  ds=0x6041A1C status=80 max_size=1524 pak_size=0
08 pak=0x6041138  ds=0x6041294 status=80 max_size=1524 pak_size=0
09 pak=0x60409B0  ds=0x6040B0C status=80 max_size=1524 pak_size=0
10 pak=0x6040228  ds=0x6040384 status=80 max_size=1524 pak_size=0
11 pak=0x603FAA0  ds=0x603FBFC status=80 max_size=1524 pak_size=0
12 pak=0x603F318  ds=0x603F474 status=80 max_size=1524 pak_size=0
13 pak=0x603EB90  ds=0x603ECEC status=80 max_size=1524 pak_size=0
14 pak=0x603E408  ds=0x603E564 status=80 max_size=1524 pak_size=0
15 pak=0x603DC80  ds=0x603DDDC status=80 max_size=1524 pak_size=0
16 pak=0x603D4F8  ds=0x603D654 status=80 max_size=1524 pak_size=0
17 pak=0x603CD70  ds=0x603CECC status=80 max_size=1524 pak_size=0
18 pak=0x603C5E8  ds=0x603C744 status=80 max_size=1524 pak_size=0
```

```
19 pak=0x603BE60  ds=0x603BFBC status=80 max_size=1524 pak_size=0
20 pak=0x603B6D8  ds=0x603B834 status=80 max_size=1524 pak_size=0
21 pak=0x603AF50  ds=0x603B0AC status=80 max_size=1524 pak_size=0
22 pak=0x603A7C8  ds=0x603A924 status=80 max_size=1524 pak_size=0
23 pak=0x603A040  ds=0x603A19C status=80 max_size=1524 pak_size=0
24 pak=0x60398B8  ds=0x6039A14 status=80 max_size=1524 pak_size=0
25 pak=0x6039130  ds=0x603928C status=80 max_size=1524 pak_size=0
26 pak=0x60389A8  ds=0x6038B04 status=80 max_size=1524 pak_size=0
27 pak=0x6038220  ds=0x603837C status=80 max_size=1524 pak_size=0
28 pak=0x6037A98  ds=0x6037BF4 status=80 max_size=1524 pak_size=0
29 pak=0x6037310  ds=0x603746C status=80 max_size=1524 pak_size=0
30 pak=0x6036B88  ds=0x6036CE4 status=80 max_size=1524 pak_size=0
31 pak=0x6036400  ds=0x603655C status=80 max_size=1524 pak_size=0
TX ring with 8 entries at 0x45790 : TLEN=3, TWD=7
tx_count = 0, tx_head = 7, tx_tail = 7
00 pak=0x000000 ds=0x600D70C status=0x38 max_size=1524 pak_size=22
01 pak=0x000000 ds=0x600D70E status=0x38 max_size=1524 pak_size=2
02 pak=0x000000 ds=0x600D70E status=0x38 max_size=1524 pak_size=2
03 pak=0x000000 ds=0x600D70E status=0x38 max_size=1524 pak_size=2
04 pak=0x000000 ds=0x600D70E status=0x38 max_size=1524 pak_size=2
05 pak=0x000000 ds=0x600D70E status=0x38 max_size=1524 pak_size=2
06 pak=0x000000 ds=0x600D70E status=0x38 max_size=1524 pak_size=2
07 pak=0x000000 ds=0x6000000 status=0x38 max_size=1524 pak_size=0
XID/Test TX desc at 0xFFFFFF, status=0x30, max_buffer_size=0, packet_size=0
XID/Test RX desc at 0xFFFFFF, status=0x0, max_buffer_size=0, packet_size=0
Status Buffer at 0x60459C8: rcv=0, tcv=0, local_state=0, remote_state=0
phase=0, tac=0, currd=0x00000, curxd=0x00000
bad_frames=0, frmrs=0, T1_timeouts=0, rej_rxs=0, runts=0
0 missed datagrams, 0 overruns, 0 bad frame addresses
0 bad datagram encapsulations, 0 user primitive errors
0 provider primitives lost, 0 unexpected provider primitives
0 spurious primitive interrupts, 0 memory errors, 0 tr
%LINEPROTO-5-UPDOWN: Linansmitter underruns
mk5025 registers: csr0 = 0x0E00, csr1 = 0x0302, csr2 = 0x0704
                  csr3 = 0x5500, csr4 = 0x0214, csr5 = 0x0008
```

Example of the show controllers serial Command for a PA-E3 Serial Port Adapter

The following is sample output from the **showcontrollersserial** command for a PA-E3 serial port adapter installed in slot 2:

```
Router# show controllers serial 2/0
M1T-E3 pa: show controller:
PAS unit 0, subunit 0, f/w version 2-55, rev ID 0x2800001, version 2
idb = 0x6080D54C, ds = 0x6080F304, ssb=0x6080F4F4
Clock mux=0x30, ucmd_ctrl=0x0, port_status=0x1
Serial config=0x8, line config=0x1B0202
maxdgram=4474, bufpool=128Kb, 256 particles
   rxLOS inactive, rxLOF inactive, rxAIS inactive
   txAIS inactive, rxRAI inactive, txRAI inactive
line state: up
E3 DTE cable, received clockrate 50071882
base0 registers=0x3D000000, base1 registers=0x3D002000
mxt_ds=0x608BA654, rx ring entries=128, tx ring entries=256
rxring=0x4B01F480, rxr shadow=0x6081081C, rx_head=26
txring=0x4B01F960, txr shadow=0x60810E48, tx_head=192, tx_tail=192, tx_count=0
throttled=0, enabled=0, disabled=0
rx_no_eop_err=0, rx_no_stp_err=0, rx_no_eop_stp_err=0
rx_no_buf=0, rx_soft_overrun_err=0, dump_err= 1
tx_underrun_err=0, tx_soft_underrun_err=0, tx_limited=0
tx_fullring=0, tx_started=11504
```

```
   Framing is g751, Clock Source is Line, Bandwidth limit is 34010.
   Scrambling is enabled
   National Bit is 0, International Bits are: 0 0
   DSU mode 1
   Data in current interval (213 seconds elapsed):
     0 Line Code Violations, 0 P-bit Coding Violation
     0 C-bit Coding Violation
     0 P-bit Err Secs, 0 P-bit Severely Err Secs
     0 Severely Err Framing Secs, 0 Unavailable Secs
     0 Line Errored Secs, 0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
   Total Data (last 24 hours)
     0 Line Code Violations, 0 P-bit Coding Violation,
     0 C-bit Coding Violation,
     0 P-bit Err Secs, 0 P-bit Severely Err Secs,
     0 Severely Err Framing Secs, 0 Unavailable Secs,
     0 Line Errored Secs, 0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
   No alarms detected.
```

Example of the show controllers serial Command for a PA-T3 Serial Port Adapter

The following is sample output from the **showcontrollersserial** command that shows serial port 1/0/0 on a 1-port PA-T3 serial port adapter installed on a VIP2 in chassis slot 1:

```
Router# show controllers serial 2/0/1
Serial1/0/0 -
   Mx T3(1) HW Revision 0x3, FW Revision 2.55
   Framing is c-bit, Clock Source is Line
   Bandwidth limit is 35000, DSU mode 1, Cable length is 50
   Data in current interval (325 seconds elapsed):
     0 Line Code Violations, 0 P-bit Coding Violation
     0 C-bit Coding Violation
     0 P-bit Err Secs, 0 P-bit Sev Err Secs
     0 Sev Err Framing Secs, 0 Unavailable Secs
     0 Line Errored Secs, 0 C-bit Errored Secs, 0 C-bit Sev Err Secs
   Total Data (last 24 hours)
     0 Line Code Violations, 0 P-bit Coding Violation,
     0 C-bit Coding Violation,
     0 P-bit Err Secs, 0 P-bit Sev Err Secs,
     0 Sev Err Framing Secs, 0 Unavailable Secs,
     0 Line Errored Secs, 0 C-bit Errored Secs, 0 C-bit Sev Err Secs
No alarms detected.
```

Example of the show controllers serial Command for a Channelized T3 SPA

The following is sample output from the **showcontrollersserial**command for a 2-port or 4-Port CT3 SPA located in slot 3 of a Cisco 7304 router:

```
Router# show controllers serial
Serial3/1/0 -
   Framing is c-bit, Clock Source is Internal
   Bandwidth limit is 44210, DSU mode 0, Cable length is 10
   rx FEBE since last clear counter 0, since reset 0
   Data in current interval (0 seconds elapsed):
     0 Line Code Violations, 0 P-bit Coding Violation
     0 C-bit Coding Violation
     0 P-bit Err Secs, 0 P-bit Sev Err Secs
     0 Sev Err Framing Secs, 0 Unavailable Secs
     0 Line Errored Secs, 0 C-bit Errored Secs, 0 C-bit Sev Err Secs
```

```
      0 Severely Errored Line Secs
      0 Far-End Errored Secs, 0 Far-End Severely Errored Secs
      0 CP-bit Far-end Unavailable Secs
      0 Near-end path failures, 0 Far-end path failures
      0 Far-end code violations, 0 FERF Defect Secs
      0 AIS Defect Secs, 0 LOS Defect Secs
    Transmitter is sending AIS.
    Receiver has loss of signal.
 Serial3/1/3 -
    Framing is c-bit, Clock Source is Line
    Bandwidth limit is 44210, DSU mode 0, Cable length is 10
    rx FEBE since last clear counter 0, since reset 0
    Data in current interval (757 seconds elapsed):
      0 Line Code Violations, 0 P-bit Coding Violation
      0 C-bit Coding Violation
      0 P-bit Err Secs, 0 P-bit Sev Err Secs
      0 Sev Err Framing Secs, 0 Unavailable Secs
      0 Line Errored Secs, 0 C-bit Errored Secs, 0 C-bit Sev Err Secs
      0 Severely Errored Line Secs
      0 Far-End Errored Secs, 0 Far-End Severely Errored Secs
      0 CP-bit Far-end Unavailable Secs
      0 Near-end path failures, 0 Far-end path failures
      0 Far-end code violations, 0 FERF Defect Secs
      0 AIS Defect Secs, 0 LOS Defect Secs
    No alarms detected.
```

The table below describes the fields shown in the **showcontrollersserial** output.

Note The fields appearing in the output will vary depending on card type, controller configuration, and the status of the controller line.

Table 76: show controllers serial Field Descriptions

Field	Description
Serial	Name of the serial controller.
Framing	Framing type.
Clock source	Source of the synchronization signal (clock).
Bandwidth limit	The allowable bandwidth for the controller.
DSU mode	The Data Service Unit (DSU) interoperability mode.
Cable length	The distance to the first repeater.
rx FEBE since last clear counter	Number of received far-end block errors. **Note** Line far-end block error (accumulated from the M0 or M1 byte) is reported when the downstream LTE detects BIP(B2) errors. Path far-end block error (accumulated from the G1 byte) is reported when the downstream PTE detects BIP(B3) errors.
rx FEBE since last reset	Number of received far-end block errors.

Field	Description
Line Code Violations	Number of Bipolar Violation (BPV) errors or Excessive Zeros (EXZ) errors.
P-bit Coding Violations	Number of P-bit errors encountered between source and destination.
C-bit coding violations	Number of C-bit errors encountered between source and destination.
P-bit Err Secs (PES)	Number of seconds with P-bit errors. **Note** A PES is a second with one or more PCVs or one or more Out of Frame defects or a detected incoming AIS. This gauge is not incremented when UASs are counted.
P-bit Sev Err Secs (PSES)	Number of seconds with P-bit severe errors. **Note** A PSES is a second with 44 or more PCVs or one or more Out of Frame defects or a detected incoming AIS. This gauge is not incremented when UASs are counted.
Sev Err Framing Secs	The number of 1-second intervals in which either a Remote Alarm Indication was received or a Loss Of Frame condition occurred.
Unavailable Secs	The number of 1-second intervals in which the controller was down.
Line Errored Secs	The number of 1-second intervals in which a Line Code Violation occurred.
C-bit Errored Secs (CES)	Number of seconds with C-bit errors. **Note** A CES is a second with one or more CCVs or one or more Out of Frame defects or a detected incoming AIS. This count is only for the SYNTRAN and C-bit Parity DS3 applications. This gauge is not incremented when UASs are counted.
C-bit Sev Err Secs (CSES)	Number of seconds with severe C-bit errors. **Note** A CSES is a second with 44 or more CCVs or one or more Out of Frame defects or a detected incoming AIS. This count is only for the SYNTRAN and C-bit Parity DS3 applications. This gauge is not incremented when UASs are counted.

Field	Description
Severely Errored Line Secs	For ESF signals, this is a second in which one of the following defects is detected: • 320 or more Path Code Violation errors. • One or more Out of Frame defects. • An AIS defect. For E1-CRC signals, this is a second with one of the following errors: • 832 or more Path Code Violation errors. • One or more Out of Frame defects. For E1-nonCRC signals, this is a second with 2048 or more Line Code Violations.
Far-End Errored Secs	Number of seconds of far-end failures.
Far-End Severely Errored Secs	The number of 1-second intervals in which either a Remote Alarm Indication was received or a Loss Of Frame condition occurred.
P-bit Unavailable Secs	Number of seconds the interface is unavailable because of P-bit errors.
CP-bit Unavailable Secs	Number of seconds the interface is unavailable because of CP-bit errors.
CP-bit Far-end Unavailable Secs	Number of seconds the interface is unavailable because of CP-bit errors from the far-end device.
Near-end path failures	Indicates the number of failures at the near end of the path, or device, during the specified trace period.
Far-end path failures	Indicates the number of failures at the remote (or far) end of the path, or device, during the specified trace period.
Far-end code violations	Indicates a frame synchronization bit error in the D4 and E1-no CRC formats, or a CRC error in the Extended Superframe (ESF) and E1-CRC formats has occurred on the remote, or far-end device.
FERF Defect Secs	Number of far-end receive failures detected per second.
AIS Defect Secs	Number of alarm indication signals per second.
LOS Defect Secs	Number of loss of signal alarms per second.
Path Code Violations	Indicates a frame synchronization bit error in the D4 and E1-no CRC formats, or a CRC error in the Extended Superframe (ESF) and E1-CRC formats.
Slip Secs	Indicates the replication or deletion of the payload bits of a domestic trunk interface (DS1) frame. A slip might happen when there is a difference between the timing of a synchronous receiving terminal and the received signal.

Field	Description
Fr Loss Secs	Indicates the number of seconds an Out of Frame (OOF) error is detected.
Line Err Secs	Line Errored Seconds (LES) is a second in which one or more Line Code Violation errors are detected.
Degraded Mins	A degraded minute is one in which the estimated error rate exceeds 1E-6 but does not exceed 1E-3.
Errored Secs	In ESF and E1-CRC links, an errored second is a second in which one of the following defects is detected: • One or more Path Code Violations. • One or more Controlled Slip events. **Note** For SF and E1 no-CRC links, the presence of Bipolar Violations also triggers an errored second.
Bursty Err Secs	A second with more than one but fewer than 320 Path Coding Violation errors, no Severely Errored Frame defects, and no detected incoming AIS defects. Controlled slips are not included in this parameter.

show controllers serial bert

To view the BERT statistics for a completed or in-progress BERT test, enter the **showcontrollersserialbert** in user EXEC or EXEC privileged mode.

show controllers serial *slot/interface-number* **bert**

Syntax Description

slot	Specifies the slot where the serial interface is located.
interface-number	Specifies the number of the serial interface.

Command Default

None

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.1(12c)EX1	This command was introduced for Cisco 7304 routers.
12.2(18)S	This command was introduced on Cisco 7304 routers running Cisco IOS Release 12.2S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is used to view the results of a user-initiated BERT test.

Examples

In the following example, the **showcontrollersserialbert**command is used to view a BERT test that is still in progress:

```
Router#
show controllers serial 6/0 bert
Interface Serial6/0 (DS3 port 1)
 BERT information:
  State            :enabled (sync'd)
  Pattern          :2^23
  Interval         :10 minutes
  Time remaining   :00:01:44
  Total errors     :0
  Time this sync   :00:08:10
  Errors this sync :0
  Sync count       :1
```

In the following example, the **showcontrollersserialbert**command is used to view a BERT test that is complete:

```
Router# show controllers serial 6/0 bert
Interface Serial6/0 (DS3 port 1)
 BERT information:
  State            :enabled (sync'd)
  Pattern          :2^23
```

```
Interval          :10 minutes
Time remaining    :00:09:44
Total errors      :0
Time this sync    :00:00:10
Errors this sync :0
Sync count        :1
```

Related Commands

Command	Description
bert errors	Inserts intention errors into a BERT test.
bert pattern	Begins a BERT test.

show controllers sm

To display controller information for the service module interface, use the **showcontrollerssm** command in user EXEC or privileged EXEC mode.

show controllers sm *slot*/*port*

Syntax Description

slot	Router slot in which the service module is installed. Range: 1 to 4.
/ *port*	Port number of the module interface. Always use 0. The slash mark (/) is required.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

The output from this command is generally useful for diagnostic tasks performed by technical support only. You can, however, use the displayed hardware statistics to obtain the receive and transmit packet statistics that are collected by the hardware controller during packet processing.

Examples

The following example shows how to display information for the SM-SRE installed in the router:

```
Router# show controllers sm 1/0
Interface SM1/0
Hardware is PSE2
HWIDB: 0x11E3C8C8 INSTANCE: 0x01323100, FASTSEND: 0x040D6C44
Init flags: 0x23

FPGA registers
----------------
  Base address:   0xE4000000    Revision:       0x09030416
  FPGA type:      0x316B6278    FPGA_error_val: 0x00000000
  Cfg MSI mask:   0x00000008    Rx_buffer_size: 0x00000600

Frame statistics: (polling enabled)
-----------------------------------
  tx_frame_cnt: 177                     rx_frame_cnt: 28
  tx_byte_cnt: 45154                    rx_byte_cnt: 2113
  tx_pause_frame_cnt: 0                 rx_pause_frame_cnt: 0
  rx_unicast_filtered_cnt: 0            rx_multicast_filtered_cnt: 8
  rx_undersize_pkts: 0                  rx_oversize_pkts: 0
  tx_64_byte_pkts: 38                   rx_64_byte_pkts: 17
  tx_65_to_127_byte_pkts: 17            rx_65_to_127_byte_pkts: 8
  tx_128_to_255_byte_pkts: 6            rx_128_to_255_byte_pkts: 3
  tx_256_to_511_byte_pkts: 116          rx_256_to_511_byte_pkts: 0
  tx_512_to_1023_byte_pkts: 0           rx_512_to_1023_byte_pkts: 0
  tx_1024_to_1518_byte_pkts: 0          rx_1024_to_1518_byte_pkts: 0
  rx_congestion_drop_cnt: 0             rx_mtusize_drop_cnt: 0
  rx_bad_cnt: 0

Interrupt statistics
--------------------
  ge_tx_interrupt: 171                  ge_rx_interrupt: 20
```

```
  txbd_seq_err: 0                      txbd_done_err: 0
  rxbd_done_err: 0                     isl_inner_crc_err: 0
  pcie_busmstr_dsbld_err: 0            pcie_tgt_abort_err: 0
  pcie_mst_abort_err: 0                spi_done_event: 0
  rx_empty_pak: 0                      rx_sw_usage_err: 0
  ing_buf_adrs_err: 0                  pcie_null_ptr_err: 0
  uart_tx_intr: 13                     uart_rx_intr: 27169
  uart_break_detected: 1               uart_framing_err: 0
  uart_bad_egr_adrs: 0                 uart_egr_overflow: 0
  i2c_errs: misc/nack/tmo: 0/0/0

TX ring
-------
  Tx Ring txr_head/txr_tail:  178/178
  Tx Shadow txs_head/txs_tail/txs_free: 178/178/256
  Tx Ring(txr): 0x3C631800 Tx Shadow (malloc): 0x01323380
  Tx Limited: 0 Tx Count: 0 hold_pak 0x00000000

RX rings
--------
  size: 256      max_spin_size 32       head: 20
  Rx Ring(rxr):   0x3C631000  rxr_malloc: 0x3C631000
  Rx Shadow(rxs): 0x11E3D6CC   rxs_malloc: 0x11E3D6CC

Software MAC Address Filter (hash:length/addr/mask/hits)
--------------------------------------------------------
   000:  0  ffff.ffff.ffff  0000.0000.0000        3
   007:  0  001e.4a97.644d  0000.0000.0000        0
   192:  0  0180.c200.0002  0000.0000.0000        0
   192:  1  0100.0ccc.cccc  0000.0000.0000        0
   197:  0  0180.c200.0007  0000.0000.0000        0

   Software filtered frames: 0
   Unicast overflow mode:   0
   Multicast overflow mode: 1
   Promiscuous mode:        0

  HW MAC Address Filter
  ---------------------
   Unicast Addr0: 001E.4A97.644D
   Unicast Addr1: 0000.0000.0100
   Unicast Addr2: 0000.0000.0100
   Unicast Addr3: 0000.0000.0100
   Unicast Addr4: 0000.0000.0100
   Unicast HW Filter Count   : 1

   Multicast Hash b63_32: 0x2000001
   Multicast Hash b32_00: 0x00
   HW unicast filter enabled: Yes
   HW multicast filter enabled: Yes

FPGA upgrade info
-----------------
  Golden area fpga version:  00000000
  Upgrade area fpga version: 09030416
  IOS bundled fpga version:  09030416
```

The table below describes the significant fields shown in the display.

Table 77: show controllers analysis-module Field Descriptions

Field	Description
Hardware	Description of the chip being used.
IDB, FASTSEND	Address in router memory of the Interface Descriptor Block (IDB) and the fastsend routine.
INSTANCE	Device-specific data stored in router memory that lists the memory locations and current indexes of receive (Rx) and transmit (Tx) rings in router I/O memory.
CONTROL AND STATUS REGISTERS (CSR)	Control and status registers that are physically located on the chip itself and that are accessed by the CPU over the Peripheral Component Interconnect (PCI) bus.
PHY REGISTERS	Contents of the PHY registers. PHY is a device that interfaces the physical Ethernet line and that is located between the chip and the physical line.
HARDWARE STATISTICS	Receive (Rx) and transmit (Tx) traffic statistics collected by the chip.
INTERRUPT STATISTICS	Transmit (Tx), Receive (Rx), control, software, and flow control interrupt statistics collected by the chip.

Related Commands

Command	Description
service-module sm status	Displays hardware and software status information about the SM-SRE.
show interfaces sm	Displays status, traffic data, and configuration information about the SM-SRE interface.

show controllers sonet

To display information about Synchronous Optical Network (SONET) controllers, use the **showcontrollerssonet** command in user EXEC or privileged EXEC mode with the appropriate parameters for the operating mode of the channelized line.

show controllers sonet[{*slot/bay/port*
[illegible]
slot/bay/port:t1-line-number}][{**bert** | **brief** | **tabular**}]

Cisco Series
show controllers sonet [*slot/bay/port*]

Syntax Description

slot / bay / port	(Optional) Slot, bay, and port number. The slash mark is required between the *slot* argument, the *bay* argument, and the *port* argument. **Note** This form of the syntax is used only for the synchronous transport module-1 (STM-1) trunk card on a Cisco AS5850 universal gateway.
slot / bay / port **.** *sts1 - number / t1 -* number	(Optional) Slot and port number of a T1 line under SONET framing in CT3 mode.
slot / bay / port **.** *vtg1 - number / sts1 - number / t1 - number*	(Optional) Slot and port number of a T1 line under SONET framing in VT-15 mode.
slot / bay / port **.** *au-3-number / tug-2-number / t1-number*	(Optional) Slot and port number of a T1 line under synchronous digital hierarchy (SDH) framing with administrative unit type 3 (AU-3) administrative unit group (AUG) mapping.
slot / bay / port **.** *au - 4 - number / tug - 3 - number / tug - 2 - number / e1 - line - number*	(Optional) Slot and port number of an E1 line under SDH framing with AU-4 AUG mapping.
slot / bay / port **.** *au - 4 - number / vc3 - number*	(Optional) Slot and port number of a DS3/E3 interface under SDH framing with AU-4 mapping.
slot / bay / port **:** *interface - number*	(Optional) Slot and port number of a DS3/E3 interface under SONET framing or SDH framing with AU-3 mapping.
t3 slot / bay / port **:** *t1 - line - number*	(Optional) Displays information for a T1 line under SF or ESF format framing.
bert	(Optional) Displays bit error rate test (BERT) information.
brief	(Optional) Displays summary information about SONET controllers.
tabular	(Optional) Displays SONET controller information in a tabular format.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.0(21)S	This command was introduced on Cisco 12000 series Internet routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T, and support was added for the STM-1 trunk card on the Cisco AS5850 platform.
12.3(11)T	This command was modified to support SONET APS on the Cisco AS5850 platform.
Cisco IOS XE Release 3.1	This command was modified to display the Detected Alarms and Asserted/Active Alarms fields.
Cisco IOS XE Everest 16.5.1	This command was implemented on the Cisco ASR 900 Series Rotuters and Cisco NCS 4200 Series.
XE Fuji 16.8.x	This command output was modified on the Cisco Series Routers to display far-end counters for performance monitoring.

Usage Guidelines

You can enter the **showcontrollerssonet** command at any time during a BERT.

Examples

The following is sample output from the **showcontrollerssonet**command on a T1 line under SONET framing in VT-15 mode. (The table below describes the lines in the BERT portion of the output.)

```
Router# show controllers sonet
 4/0.1/1/1 brief
OC3.STS1 4/0.1 is up. Hardware is GSR 2 port STM1/OC3 (channelized)
  Applique type is VT1.5 in STS-1

 STS-1 1, VTG 1, T1 1 (VT1.5 1/1/1) is up
  timeslots: 1-24
  FDL per AT&T 54016 spec.
  No alarms detected.
  Framing is ESF, Clock Source is Internal
  BERT test result (running)
     Test Pattern : 2^20-QRSS, Status : Sync, Sync Detected : 1
     Interval : 5 minute(s), Time Remain : 4 minute(s)
     Bit Errors (since BERT started): 0 bits,
     Bits Received (since BERT started): 112 Mbits
     Bit Errors (since last sync): 0 bits
     Bits Received (since last sync): 112 Mbits
```

Table 78: show controllers sonet Line Descriptions

Field	Description
BERT test result (running)	Indicates the current state of the test. In this case, “running” indicates that the test is still active. If the test is complete, “done” is displayed.
Test Pattern : 2^20-QRSS, Status : Sync, Sync Detected : 1	Indicates the test pattern that you selected for the test (2^20-QRSS), the current synchronization state (Sync), and the number of times that synchronization was detected during this test (1).

Field	Description
Interval : 5 minute(s), Time Remain : 4 minute(s)	Indicates the time allocated for the test to run and the time remaining for the test to run. For a BERT that you terminate before the time expires, this line indicates the time the test would have taken to run and the time remaining for the test to run had you not terminated it. “unable to complete” is displayed to indicate that you interrupted the test.
Bit Errors (since BERT started): 0 bits Bits Received (since BERT started): 112 Mbits Bit Errors (since last sync): 0 bits Bits Received (since last sync): 112 Mbits	Shows the bit errors that were detected versus the total number of test bits that were received since the test started and since the last synchronization was detected.

The following is sample output from the **showcontrollerssonet**command for an E1 line under SDH framing with AU-4 AUG mapping.

```
Router# show controllers sonet 3/0.1/1/3/5
SONET 3/0 is up. (Configured for Locally Looped)  Hardware is GSR 2 port
STM1/OC3 (channelized)
  Applique type is Channelized OCx interface
  Clock Source is Line, AUG mapping is AU4.
Medium info:
  Type: SDH, Line Coding: NRZ, Line Type: Short SM
Regenerator Section:
LOF = 0          LOS = 0                           BIP(B1) = 0
Multiplex Section:
  AIS = 0          RDI = 0          REI = 0          BIP(B2) = 0
Active Defects: None
Active Alarms: None
Alarm reporting enabled for: SF SLOS SLOF B1-TCA B2-TCA B3-TCA
BER thresholds:  SF = 10e-3  SD = 10e-6
TCA thresholds:  B1 = 10e-6  B2 = 10e-6  B3 = 10e-6
High Order Path:

PATH 1:
  AIS = 0          RDI = 0          REI = 15         BIP(B3) = 11
  LOP = 0          PSE = 4          NSE = 0          NEWPTR = 1
  LOM = 0          PLM = 0          UNEQ = 0
Active Defects: None

S1S0 = 02, C2 = 02

PATH TRACE BUFFER : STABLE
CRC-7: 0xF2 OK
  52 6F 75 74 65 72 33 2F  30 2F 31 00 00 00 00       Router3/0/1....

 STM1.AU4 3/0.1 is up.  Hardware is GSR 2 port STM1/OC3 (channelized)
  Applique type is C12 in TUG-3 in AU-4

 AU-4 1, TUG-3 1, TUG-2 1, E1 1 (C-12 1/1/1/1) is up
  timeslots: 1-31
  No alarms detected.
  Framing is crc4, Clock Source is Internal
  BERT test result (running)
     Test Pattern : 2^15, Status : Sync, Sync Detected : 1
```

```
     Interval : 5 minute(s), Time Remain : 5 minute(s)
     Bit Errors (since BERT started): 0 bits,
     Bits Received (since BERT started): 95 Mbits
     Bit Errors (since last sync): 0 bits
     Bits Received (since last sync): 95 Mbits
  Data in current interval (708 seconds elapsed):
     0 Line Code Violations, 1 Path Code Violations
     0 Slip Secs, 1 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     1 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
     0 Unavail Secs, 0 Stuffed Secs
  Data in Interval 1:
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
     0 Unavail Secs, 0 Stuffed Secs
  Data in Interval 2:
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
     0 Unavail Secs, 0 Stuffed Secs
  Data in Interval 3:
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 1 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     1 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
     0 Unavail Secs, 0 Stuffed Secs
  Total Data (last 3 15 minute intervals):
     0 Line Code Violations,0 Path Code Violations,
     0 Slip Secs, 1 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins,
     1 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
     0 Unavail Secs, 0 Stuffed Secs
```

The following is sample output from the **showcontrollerssonet**command when AUG mapping is AU-3 and the **tabular** keyword is specified.

```
Router# show controllers sonet
 2/0.1/1/1 tabular
SONET 2/0/0 is up.
Channelized OC-3/STM-1 SMI PA
  H/W Version : 0.2.3, ROM Version : 1.2
  FREEDM version : 2, F/W Version : 0.14.0
SONET 2/0/0   E1   1/1/1 is down
  Transmitter is sending LOF Indication (RAI).
  Receiver has loss of frame.
  Framing is crc4, Clock Source is internal, National bits are 0x1F.
  INTERVAL      LCV   PCV   CSS  SEFS   LES    DM    ES   BES   SES   UAS    SS
  17:26-17:29     0     0     0     0     0     0     0     0     0   173     0
  17:11-17:26     0     0     0     0     0     0     0     0     0   471     0
  16:56-17:11     0     0     0     0     0     0     0     0     0     0     0
  16:41-16:56     0     0     0     0     0     0     0     0     0     0     0
  16:26-16:41     0     0     0     0     0     0     0     0     0   216     0
  16:11-16:26     0     0     0     0     0     0     0     0     0   225     0
  Total           0     0     0     0     0     0     0     0     0   912     0
```

The following is partial sample output from the **showcontrollerssonet** command using an STM-1 card in the Cisco AS5850.

```
Router# show controllers sonet 3/0
SONET 3/0 is down.
  Applique type is Channelized Sonet/SDH
  Clock Source is Internal, AUG mapping is AU4.
Medium info:
  Type: SDH, Line Coding: NRZ, Line Type: Short SM
Regenerator Section Status:
```

```
  LOS
Multiplex Section Status:
Higher Order Path Status:
  Path# 1 has no defects
Lower Order Path Status:
  VC-12 1/1/1/1 has no defects
  VC-12 1/1/1/2 has no defects
  VC-12 1/1/1/3 has no defects
  VC-12 1/1/2/1 has no defects
  VC-12 1/1/2/2 has no defects
  VC-12 1/1/2/3 has no defects
  VC-12 1/1/3/1 has no defects
  VC-12 1/1/3/2 has no defects
  VC-12 1/1/3/3 has no defects
  VC-12 1/1/4/1 has no defects
  VC-12 1/1/4/2 has no defects
  VC-12 1/1/4/3 has no defects
  VC-12 1/1/5/1 has no defects
  VC-12 1/1/5/2 has no defects
  VC-12 1/1/5/3 has no defects
  VC-12 1/1/6/1 has no defects
  VC-12 1/1/6/2 has no defects
  .
  .
  .
  VC-12 1/3/5/3 has no defects
  VC-12 1/3/6/1 has no defects
  VC-12 1/3/6/2 has no defects
  VC-12 1/3/6/3 has no defects
  VC-12 1/3/7/1 has no defects
  VC-12 1/3/7/2 has no defects
  VC-12 1/3/7/3 has no defects
  Data in current interval (20 seconds elapsed):
   Regenerator Section:
     0 CVs, 20 ESs, 20 SESs, 0 SEFSs
   Multiplex Section:
     0 CVs, 0 ESs, 0 SESs, 0 UASs
   Higher Order Path:
     Path# 1:  0 CVs, 0 ESs, 0 SESs, 20 UASs
   Lower Order Path:
     VC-12 1/1/1/1:  0 CVs, 0 ESs, 0 SESs, 20 UASs
     VC-12 1/1/1/2:  0 CVs, 0 ESs, 0 SESs, 20 UASs
     VC-12 1/1/1/3:  0 CVs, 0 ESs, 0 SESs, 20 UASs
     VC-12 1/1/2/1:  0 CVs, 0 ESs, 0 SESs, 20 UASs
     VC-12 1/1/2/2:  0 CVs, 0 ESs, 0 SESs, 20 UASs
     VC-12 1/1/2/3:  0 CVs, 0 ESs, 0 SESs, 20 UASs
     .
     .
     .
     VC-12 1/3/5/3:  0 CVs, 0 ESs, 0 SESs, 20 UASs
     VC-12 1/3/6/1:  0 CVs, 0 ESs, 0 SESs, 20 UASs
     VC-12 1/3/6/2:  0 CVs, 0 ESs, 0 SESs, 20 UASs
     VC-12 1/3/6/3:  0 CVs, 0 ESs, 0 SESs, 20 UASs
     VC-12 1/3/7/1:  0 CVs, 0 ESs, 0 SESs, 20 UASs
     VC-12 1/3/7/2:  0 CVs, 0 ESs, 0 SESs, 20 UASs
     VC-12 1/3/7/3:  0 CVs, 0 ESs, 0 SESs, 20 UASs
```

The table below describes the significant fields shown in the display.

Table 79: show controllers sonet STM-1 Field Descriptions

Field	Description
SONET 3/0	The SONET controller in slot 3 shows the state in which it is operating. The controller's state can be up, down, or administratively down. Loopback conditions are shown by (Locally Looped) or (Remotely Looped).
Applique type	Controller type.
Clock Source	User-specified clock source (Line or Internal).
AUG mapping	Indicates type of administrative unit group (AUG) mapping.
Line Coding	Shows the current line encoding type, either return to zero (RZ) or non return to zero (NRZ).
Line Type	Line type for this interface. Optical line types can be either long range (LONG) or short range (SHORT), and either single mode (SM) or multimode (MM).
VC-12	Indicates the number of the virtual circuit (VC) and whether the VC has reported any defects.
CVs	Number of coding violation (CV) error events.
ESs	An errored second (ES) is a second in which one of the following is detected: • One or more path code violations. • One or more out of frame defects. • One or more controlled slip events. • A detected alarm indication signal (AIS) defect.
SESs	Severely errored seconds (SESs) are seconds with one or more out-of-frame defects or a detected incoming AIS. This gauge is not incremented when UASs are counted.
SEFSs	Severely errored framing seconds (SEFSs) are seconds with one or more out-of-frame defects or a detected incoming AIS.
UASs	Unavailable seconds (UASs) are calculated by counting the number of seconds for which the interface is unavailable.

The following is partial output from the **showcontrollerssonet**command using an STM-1 card in the Cisco AS5850 with SONET APS configured.

```
Router# show controllers sonet 1/0
SONET 1/0 is up.
  Applique type is Channelized Sonet/SDH
  Clock Source is Line, AUG mapping is AU4.
  MSP 1+1 bi-directional enabled
  Protection fiber (Port 0), No Alarm, traffic in-use
  Working fiber (Port 1), No Alarm, traffic not in-use
  Local request: No Request
  Remote request: No Request
Medium info:
  Type: SDH, Line Coding: NRZ, Line Type: Short SM
Regenerator Section Status:
```

```
  No alarms detected.
Multiplex Section Status:
  No alarms detected.
  No BER failure/degrade detected
  B2 BER_SF threshold power : 3
  B2 BER_SD threshold power : 6
Higher Order Path Status:
  Path# 1 has no defects
Lower Order Path Status:
  VC-12 1/1/1/1 has no defects
  VC-12 1/1/1/2 has no defects
  VC-12 1/1/1/3 has no defects
  .
  .
  .
```

The table below describes the significant fields shown in the display that are different from the fields described in the table above.

Table 80: show controllers sonet STM-1 APS Field Descriptions

Field	Description
MSP 1+1	Indicates whether the SDH multiplex section protection (MSP) is bidirectional or unidirectional.
Protection fiber	Indicates the port location of the protect fiber, whether an alarm has been detected, and whether traffic is flowing through the port.
Working fiber	Indicates the port location of the working fiber, whether an alarm has been detected, and whether traffic is flowing through the port.
Local request	Indicates whether a local request to switch fibers has been received. If a request has been received, the type of request (forced, lockout, or manual) is indicated.
Remote request	Indicates whether a remote request to switch fibers has been received. If a request has been received, the type of request (forced, lockout, or manual) is indicated.
No alarms detected	Alarms detected by the controller are displayed here. The possible alarms are as follows: • Transmitter is sending remote alarm. • Transmitter is sending alarm indication signal (AIS). • Receiver has loss of signal. • Receiver is getting AIS. • Receiver has loss of frame. • Receiver has remote alarm. • Receiver has no alarms.
No BERT failure/degrade detected	No bit error rate (BER) failures or degrades detected.

Field	Description
B2 BER_SF threshold power	BER signal failure (SF) threshold configured with the **b2sf-ber** controller command.
B2 BER_SD threshold power	BER signal degrade (SD) threshold configured with the **b2sd-ber** controller command.

The following is a sample output from the **showcontrollerssonet**command using the CHOCX card.

```
Router# show controllers sonet 0/0/0

SONET 0/0/0 is down.
  Hardware is SPA-1XCHOC12/DS0
 Applique type is Channelized Sonet/SDH
 Clock Source is Line
Medium info:
  Type: Sonet, Line Coding: NRZ,
 SECTION:
  LOS = 1          LOF = 0                           BIP(B1) = 0
 SONET/SDH Section Tables
  INTERVAL       CV    ES   SES  SEFS
  18:51-18:54     0   182   182   182   LINE:
  AIS = 0          RDI = 0          REI = 0          BIP(B2) = 0
Active Defects: None
Detected Alarms: PRDI B3-TCA
Asserted/Active Alarms: PRDI B3-TCA
 Alarm reporting enabled for: PLOP LOM B3-TCA
BER thresholds:  SF = 10e-3  SD = 10e-6
TCA thresholds:  B1 = 10e-6  B2 = 10e-6
```

The table below describes the significant fields shown in the display.

Table 81: show controllers sonet CHOCX Card Field Descriptions

Field	Description
Applique type	The controller type.
Clock Source	The user-specified clock source (line or internal).
Active Defects	List of active SONET defects.
Detected Alarms	List of alarms detected by the controllers.
Asserted/Active Alarms	List of resultant active alarms after SONET alarm hierarchy is enforced on detected alarms.
BER thresholds	BER threshold values of the specified alarms.
TCA thresholds	Threshold crossing alarm (TCA) values of the specified alarms.

The following is sample output from the **showcontrollerssonet**command using a shared port adapter (SPA), SPA-1XCHOC12/DS0 on a Cisco 7600 series router. SPAs such as the SPA-1XCHSTM1/OC3, SPA-1xCE-OC3/STM1, and SPA-1xCHOC12/OC3 are also used on a Cisco 7600 series router to get output on the SONET controller.

```
Router# show controllers sonet 3/0/0.2/1
SONET 3/0/0 is up.
   Hardware is SPA-1XCHOC12/DS0
  Applique type is Channelized Sonet/SDH
  Clock Source is Line, AUG mapping is AU4.
 Medium info:
   Type: SDH, Line Coding: NRZ,
  Regenerator Section:
   LOS = 0          LOF = 0                          BIP(B1) = 0

SONET/SDH Section Tables
   INTERVAL       CV    ES   SES  SEFS
   16:07-16:12     0     0     0     0

 Multiplex Section:
   AIS = 0          RDI = 0          REI = 358160     BIP(B2) = 0
 Active Defects: None
 Detected Alarms: None
 Asserted/Active Alarms: None
 Alarm reporting enabled for: SLOS SLOF SF B1-TCA B2-TCA
 BER thresholds:  SF = 10e-3  SD = 10e-6
 TCA thresholds:  B1 = 10e-6  B2 = 10e-6
 Rx: S1S0 = 00
     K1 = 00,   K2 = 00
     J0 = 19

 Tx: S1S0 = 02
     K1 = 00,   K2 = 00
     J0 = 01
 SONET/SDH Line Tables
   INTERVAL       CV    ES   SES   UAS
   16:08-16:14     0     0     0     0
PATH 4:
  AIS = 0          RDI = 0          REI = 0          BIP(B3) = 0
  LOP = 0          PSE = 0          NSE = 0          NEWPTR = 0
  LOM = 0          PLM = 0          UNEQ = 0
Active Defects: None
Detected Alarms: None
Asserted/Active Alarms: None
Alarm reporting enabled for: PLOP LOM B3-TCA
TCA threshold:  B3 = 10e-6
Rx: C2 = 02
Tx: C2 = 02
```

The table below describes the significant fields shown in the display.

Table 82: show controllers sonet SPA Field Descriptions

Field	Description
Applique type	The controller type.
Clock Source	The user-specified clock source (line or internal).
Active Defects	List of active SONET defects.
Detected Alarms	List of alarms detected by the controllers.
Asserted/Active Alarms	List of resultant active alarms after SONET alarm hierarchy is enforced on detected alarms.

Field	Description
BER thresholds	BER threshold values of the specified alarms.
TCA thresholds	TCA values of the specified alarms.

Related Commands

Command	Description
xconnect	Configures a pseudowire for transporting data over the network.

Series Router

The following is sample output from the **show controllers sonet** command on the Cisco series routers:

```
Router# show controllers sonet 0/3/3
SONET 0/3/3 is up. ======> this is the controller/port
status.
Hardware is asr900
Port configured rate: OC3 =======> this is the rate the port is configured
on it.
Applique type is Channelized Sonet / SDH
Clock Source is Line ===> the clocking config
Medium info:
Type: Sonet, Line Coding: NRZ,
SECTION:
LOS = 0 LOF = 0 =======> the section level alarm
counter (from last clear counters)
SONET/SDH Section Tables
INTERVAL CV ES SES SEFS
05:50-05:58 0 0 0 0 ===> PMON for the
port
LINE:
AIS = 0 RDI = 0 REI = 0 BIP(B2) = 0 =======> the line level
alarm counter (from last clear counters)
Active Defects: None
Detected Alarms: None
Asserted/Active Alarms: None =========> present active
alarms on the port.
Alarm reporting enabled for: SLOS SLOF SF B2-TCA
BER thresholds: SF = 10e-3 SD = 10e-6 ====> ber thresholds
TCA thresholds: B2 = 10e-6
Rx: S1S0 = 00
K1 = 00, K2 = 00 ===> k1k2 values
J0 = 00
RX S1 = 00
Tx: S1S0 = 00
K1 = 00, K2 = 00
J0 = 00
High Order Path:
PATH 1:
Clock Source is internal ====> path level clock
AIS = 0 RDI = 0 REI = 0 BIP(B3) = 0 ======> path layer alarms counter
LOP = 0 PSE = 0 NSE = 0 NEWPTR = 0
LOM = 0 PLM = 0 UNEQ = 0
Active Defects: None
Detected Alarms: None
Asserted/Active Alarms: None ======> present alarms on the path.
```

```
Alarm reporting enabled for: PLOP LOM B3-TCA
TCA threshold: B3 = 10e-6
Rx: C2 = 00 =====> rx and tx C2 byte..
Tx: C2 = 02
PATH TRACE BUFFER : UNSTABLE
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ====> path trace of the path
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
SONET Path Tables
INTERVAL CV ES SES UAS
05:58-05:58 0 0 0 0
PATH 2:
Clock Source is internal
AIS = 0 RDI = 0 REI = 0 BIP(B3) = 0
LOP = 0 PSE = 0 NSE = 0 NEWPTR = 0
LOM = 0 PLM = 0 UNEQ = 0
Active Defects: None
Detected Alarms: None
Asserted/Active Alarms: None
Alarm reporting enabled for: PLOP LOM B3-TCA
TCA threshold: B3 = 10e-6
Rx: C2 = 00
Tx: C2 = 00
PATH TRACE BUFFER : UNSTABLE
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
SONET/SDH Path Tables
INTERVAL CV ES SES UAS
05:58-05:58 0 0 0 0
OC3.STS1 0/3/3.1 is up. ======> present status of the path
Hardware is
Applique type is VT1.5 =====> mode of the path
STS-1 1, VTG 1, T1 1 (VT1.5 1/1/1) is down ====> status of the SPE (t1)
VT Receiver has no alarm.
Receiver is getting AIS. ===> alarm of the SPE (t1)
Framing is unframed, Clock Source is Internal =====> framing of the T1, clock of the t1
Data in current interval (0 seconds elapsed):
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
0 Unavail Secs, 0 Stuffed Secs
STS-1 1, VTG 1, T1 2 (VT1.5 1/1/2) is down
VT Receiver has no alarm.
Receiver is getting AIS.
```

Series Router

The following is sample output from the **show controllers sonet tabular** command on the Cisco series routers:

```
Router# show controllers sonet 0/2/0
SONET 0/2/0 is up.
Hardware is -1T8S-10CS
Port configured rate: OC3
Applique type is Channelized Sonet
Clock Source is Internal
Medium info:
Type: Sonet, Line Coding: NRZ,
```

```
Alarm Throttling: OFF
SECTION:
LOS = 0 LOF = 0 BIP(B1) = 0
SONET Section Tables
INTERVAL CV ES SES SEFS
12:00-12:07 0 0 0 0
11:45-12:00 15 1 0 0
Total of Data in Current and Previous Intervals
11:45-12:07 15 1 0 0
LINE:
AIS = 0 RDI = 0 REI = 0 BIP(B2) = 0
Active Defects: None
Detected Alarms: None
Asserted/Active Alarms: None
Alarm reporting enabled for: SLOS SLOF LAIS SF SD LRDI B1-TCA B2-TCA
BER thresholds: SF = 10e-3 SD = 10e-6
TCA thresholds: B1 = 10e-6 B2 = 10e-6
Rx: S1S0 = 00
K1 = 00, K2 = 00
J0 = 00
RX S1 = 00
Tx: S1S0 = 00
K1 = 00, K2 = 00
J0 = 04
Tx J0 Length : 64
Tx J0 Trace :
52 6F 75 74 65 72 20 20 20 20 20 20 20 20 20 20 Router
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 00 00 ..
Expected J0 Length : 64
Expected J0 Trace :
52 6F 75 74 65 72 20 20 20 20 20 20 20 20 20 20 Router
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 00 00 ..
Rx J0 Length : 64
Rx J0 Trace :
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 ................
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 ................
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 ................
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 00 ................
SONET Line Tables
INTERVAL CV ES SES UAS CVFE ESFE SESFE UASFE
12:00-12:07 0 0 0 0 0 0 0 0
11:45-12:00 48 1 0 0 53 1 0 0
Total of Data in Current and Previous Intervals
11:45-12:07 48 1 0 0 53 1 0 0
High Order Path:
PATH 2:
Clock Source is internal
AIS = 0 RDI = 0 REI = 0 BIP(B3) = 0
LOP = 1 PSE = 0 NSE = 0 NEWPTR = 0
LOM = 0 PLM = 0 UNEQ = 1
Active Defects: None
Detected Alarms: PLOP
Asserted/Active Alarms: PLOP
Alarm reporting enabled for: PAIS PRDI PUNEQ PLOP PPLM LOM B3-TCA
TCA threshold: B3 = 10e-6
Rx: C2 = 00
Tx: C2 = 04
Tx J1 Length : 64
Tx J1 Trace
52 6F 75 74 65 72 20 30 2F 32 2F 30 2E 32 00 00 Router 0/2/0.2..
```

```
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
Expected J1 Length : 64
Expected J1 Trace
52 6F 75 74 65 72 20 30 2F 32 2F 30 2E 32 00 00 Router 0/2/0.2..
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
PATH TRACE BUFFER : UNSTABLE
Rx J1 Length : 0
Rx J1 Trace
SONET Path Tables
INTERVAL CV ES SES UAS CVFE ESFE SESFE UASFE
12:00-12:07 0 0 0 409 0 0 0 0
11:45-12:00 0 0 0 900 0 0 0 0
Total of Data in Current and Previous Intervals
11:45-12:07 0 0 0 1309 0 0 0 0
```

Related Commands

show controllers t1

To display information about the T1 links and to display the hardware and software driver information for the T1 controller, use the **showcontrollerst1** command in privileged EXEC mode.

Standard Syntax
show controllers t1 *number* [**bert**]

Cisco 7500 Series
show controllers t1 [*slot*/*port*] [**bert**]

Cisco AS5800 Access Servers
show controllers t1 *dial-shelf*/*slot*/*t3-port*:*t1-num* [**bert**]

Cisco Series
show controllers t1 [*slot*/*bay*/*port*]

Syntax Description

number	Network processor number (NPM)) number, in the range 0 through 2.
slot / *port*	(Optional) Backplane slot number and port number on the interface. Refer to your hardware installation manual for the specific slot and port numbers.
slot / *bay* / *port*	Slot number, interface module number in which the slot is inserted, and port number (Cisco series routers).
dial-shelf	Dial shelf chassis in the Cisco AS5800 access server that contains the CT3 interface card.
/ *slot*	Location of the CT3 interface card in the dial shelf chassis.
/ *t3-port*	T3 port number. The only valid value is 0.
: *t1-num*	T1 time slot in the T3 line. The value can be from 1 to 28.
bert	(Optional) Type **bert** to get a specific display for the bit-error rate testing (BERT) results. Otherwise, the display will include all other non-BERT information.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.0(2)XD	The keyword **bert** was added.
12.0(3)T	This command was implemented on the Cisco AS5800 access server.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Release	Modification
XE Everest 16.5.1	This command was implemented on the Cisco ASR 900 Series and Cisco NCS 4200 Series Routers.
XE Fuji 16.8.x	This command output was modified on the Cisco Series Routers to display far-end counters for performance monitoring.

Usage Guidelines

This command displays controller status that is specific to the controller hardware. The information displayed is generally useful for diagnostic tasks performed by technical support personnel. Use the **showcontrollerst1bert** command to display the results of the BERT feature.

The NPM or MultiChannel Interface Processor (MIP) can query the port adapters to determine their current status. Issue a **showcontrollerst1** command to display statistics about the T1 link.

If you specify a slot and port number, each 15-minute period will be displayed.

Cisco 7500 Series Routers

The following is sample output from the **showcontrollerst1** command on the Cisco 7500 series routers:

```
Router# show controllers t1
T1 4/1 is up.
  No alarms detected.
  Framing is ESF, Line Code is AMI, Clock Source is line
  Data in current interval (10 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations 0 Slip Secs, 0 Fr Loss Secs,
     0 Line Err Secs, 0 Degraded Mins 0 Errored Secs, 0 Bursty Err Secs,
     0 Severely Err Secs, 0 Unavail Secs
  Total Data (last 79 15 minute intervals):
     0 Line Code Violations, 0 Path Code Violations, 0 Slip Secs, 0 Fr Loss Secs,
     0 Line Err Secs, 0 Degraded Mins, 0 Errored Secs, 0 Bursty Err Secs,
     0 Severely Err Secs, 0 Unavail Secs
```

The table below describes the fields shown in the display.

Table 83: show controllers t1 Field Descriptions--Cisco 7500 Series

Field	Description
T1 4/1 is up	The T1 controller 1 in slot 4 is operating. The controller’s state can be up, down, or administratively down. Loopback conditions are shown by (Locally Looped) or (Remotely Looped).

Field	Description
No alarms detected	Any alarms detected by the controller are displayed here. Possible alarms are as follows: • Transmitter is sending remote alarm. • Transmitter is sending AIS. • Receiver has loss of signal. • Receiver is getting AIS. • Receiver has loss of frame. • Receiver has remote alarm. • Receiver has no alarms.
Data in current interval (10 seconds elapsed)	Shows the current accumulation period, which rolls into the 24-hour accumulation every 15 minutes. Accumulation period is from 1 to 900 seconds. The oldest 15-minute period falls off the back of the 24-hour accumulation buffer.
Line Code Violations	Indicates the occurrence of either a Bipolar Violation (BPV) or Excessive Zeros (EXZ) error event.
Path Code Violations	Indicates a frame synchronization bit error in the D4 and E1-no-CRC formats, or a CRC error in the ESF and E1-CRC formats.
Slip Secs	Indicates the replication or deletion of the payload bits of a DS1 frame. A slip may be performed when there is a difference between the timing of a synchronous receiving terminal and the received signal.
Fr Loss Secs	Indicates the number of seconds an out-of-frame error is detected.
Line Err Secs	Line Errored Seconds (LES) is a second in which one or more Line Code Violation errors are detected.
Degraded Mins	Degraded Minute is one in which the estimated error rate exceeds 1E-6 but does not exceed 1E-3.
Errored Secs	In ESF and E1-CRC links, an Errored Second is a second in which one of the following are detected: one or more Path Code Violations; one or more out-of-frame defects; one or more Controlled Slip events; a detected AIS defect. For D4 and E1-no-CRC links, the presence of Bipolar Violations also triggers an Errored Second.
Bursty Err Secs	Second with fewer than 320 and more than 1 Path Coding Violation error, no Severely Errored Frame defects and no detected incoming AIS defects. Controlled slips are not included in this parameter.

Field	Description
Severely Err Secs	For ESF signals, a second with one of the following errors: 320 or more Path Code Violation errors; one or more out-of-frame defects; a detected AIS defect. For E1-CRC signals, a second with one of the following errors: 832 or more Path Code Violation errors; one or more out-of-frame defects. For E1-no-CRC signals, a second with 2048 Line Code Violations or more. For D4 signals, a count of 1-second intervals with Framing Errors, or an Out-of-Frame defect, or 1544 Line Code Violations.
Unavail Secs	Count of the total number of seconds on the interface.

Cisco AS5800 Access Server

The following example shows the status of the T1 controllers connected to the Cisco AS5800 access servers:

```
Router# show controllers t1 1/0/0:1
T1 1/0/0:1 is up.
 No alarms detected.
 Framing is ESF, Line Code is AMI, Clock Source is Line.
 Data in current interval (770 seconds elapsed):
     5 Line Code Violations, 8 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 7 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 7 Unavail Secs
 Total Data (last 81 15 minute intervals):
     7 Line Code Violations, 4 Path Code Violations,
     6 Slip Secs, 20 Fr Loss Secs, 2 Line Err Secs, 0 Degraded Mins,
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 2 Unavail Secs
T1 1/0/1:5 is down.
 Transmitter is sending remote alarm.
 Receiver has loss of frame.
 Framing is SF, Line Code is AMI, Clock Source is Line.
 Data in current interval (770 seconds elapsed):
     50 Line Code Violations, 5 Path Code Violations
     0 Slip Secs, 7 Fr Loss Secs, 7 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 7 Unavail Secs
 Total Data (last 81 15 minute intervals):
     27 Line Code Violations, 22 Path Code Violations,
     0 Slip Secs, 13 Fr Loss Secs, 13 Line Err Secs, 0 Degraded Mins,
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 13 Unavail Secs
```

The table below describes the fields shown in the display.

Table 84: show controllers t1 Field Descriptions--Cisco AS5800 Access Server

Field	Description
T1 ... is up	Status of T1 line.
No alarms detected	Access server received no alarms.
Framing is ...	Standard T1 framing type. In this example, the framing is Extended Super Frame (ESF).

Field	Description
Line Code is ...	Standard T1 line-coding format. In this example, the line-coding format is Alternate Mark Inversion (AMI).
Clock Source is ...	Source of the synchronization signal (clock). In this example, the line is providing the clock signal.
Data in current interval ...	Summary statistics for T1 signal quality for the current time interval of 900 seconds. In this example, the statistics are for current partial interval (770 seconds of 900 seconds).
Line Code Violations	Number of T1 line code violations for the current interval.
Path Code Violations	Number of T1 path code violations for the current interval.
Slip Secs	Number of seconds in this interval during which a frame misalignment occurred.
Fr Loss Secs	Number of seconds in this interval during which frame loss occurred.
Line Err Secs	Number of seconds in this interval during which line errors occurred.
Degraded Mins	Number of minutes in this interval during which the signal quality was degraded.
Errored Secs	Number of seconds in this interval during which an error was reported.
Bursty Err Secs	Number of bursty error seconds in this interval.
Severely Err Secs	Number of severely errored seconds in this interval.
Unavail Secs	Number of unavailable seconds in this interval.
Total Data (last ... 15 minute intervals)	Summary statistics for T1 signal quality for 15-minute intervals. Every 24 hours (96 intervals) the counters in this data block clear.

Using the bert Keyword

The following is sample output from the **showcontrollerst1bert** command displaying the BERT status for all ports:

```
Router#
show controllers t1 bert
 Controller T1 0 Profile default : The Test was aborted by User
 Controller T1 0 Profile 2 : Test Never Ran
 Controller T1 1 Profile 3 : Test Never Ran
 Controller T1 1 Profile 3 : Test Failed with a BER of 10^-2
 Controller T1 2 Profile 3 : Current running, BER 0
 Controller T1 2 Profile 2 : Passed with a BER of 0
 Controller T1 3 Profile default : Test Never Ran
 Controller T1 3 Profile 2 : Test Never Ran
 Controller T1 4 Profile default : Test Never Ran
 Controller T1 4 Profile 2 : Test Never Ran
 Controller T1 5 Profile default : Test Never Ran
```

```
 Controller T1 5 Profile 2 : Test Never Ran
 Controller T1 6 Profile default : Test Never Ran
 Controller T1 6 Profile 2 : Test Never Ran
 Controller T1 7 Profile default : Test Never Ran

Controller T1 7 Profile 2 : Test Never Ran
```

The following is sample output from the **showcontrollerst1bert** command with only one T1 port, port 0.

```
Router#
show controllers t1 0 bert
Controller T1 0 Profile default : The Test was aborted by User
Controller T1 0 Profile 2 : Test Never Ran
```

Series Router

The following is sample output from the **show controllers t1** command on the Cisco series routers:

```
Router# show controllers t1 0/2/1
T1 0/2/1 is down.
Applique type is -48T1E1-CE
Cablelength is short 110
No alarms detected.
alarm-trigger is not set
Soaking time: 3, Clearance time: 10
AIS State:Clear LOS State:Clear LOF State:Clear
Framing is ESF, FDL is ansi, Line Code is B8ZS, Clock Source is Line.
BER thresholds: SF = 10e-3 SD = 10e-6
Data in current interval (230 seconds elapsed):
Near End
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavailable Secs
0 Path Failures, 0 SEF/AIS Secs
Far End
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavailable Secs
0 Path Failures
Data in Interval 1:
Near End
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 14 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 15 Unavailable Secs
1 Path Failures, 0 SEF/AIS Secs
Far End Data
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 4 Fr Loss Secs, 2 Line Err Secs, 0 Degraded Mins
4 Errored Secs, 0 Bursty Err Secs, 4 Severely Err Secs, 0 Unavailable Secs
0 Path Failures
Total Data (last 1 15 minute intervals):
Near End
0 Line Code Violations, 0 Path Code Violations,
0 Slip Secs, 0 Fr Loss Secs, 14 Line Err Secs, 0 Degraded Mins,
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 15 Unavailable Secs
1 Path Failures, 0 SEF/AIS Secs
Far End
0 Line Code Violations, 0 Path Code Violations,
0 Slip Secs, 4 Fr Loss Secs, 2 Line Err Secs, 0 Degraded Mins,
```

```
4 Errored Secs, 0 Bursty Err Secs, 4 Severely Err Secs, 0 Unavailable Secs
0 Path Failures
```

show controllers t1 bert

To get the results of the bit-error rate testing (BERT) run for all ports, use the **showcontrollerst1bert**command in privileged EXEC mode.

show **controllers** *type* [*controller-number*] [**bert**]

Syntax Description

type	Specify either T1 or E1 facility.
controller-number	(Optional) Select a specific controller/port numbers. The range is 0 to 7. If not selected, the display will show all ports.
bert	(Optional) Type **bert** to get a specific display for the BERT results. Otherwise, the display will include all other non-BERT information.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(2)XD	This command was introduced.
12.0(3)T	This command was modified.
12.2(15)T	This command is no longer supported in Cisco IOS Mainline or Technology-based releases. It may conintue to appear in Cisco IOS 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **showcontrollers** command to display the results of the BERT feature.

Examples

The following example shows how the **showcontrollers** command is used to display the BERT status for all ports:

```
Router#
show controllers t1 bert
 Controller T1 0 Profile default : The Test was aborted by User
 Controller T1 0 Profile 2 : Test Never Ran
 Controller T1 1 Profile 3 : Test Never Ran
 Controller T1 1 Profile 3 : Test Failed with a BER of 10^-2
 Controller T1 2 Profile 3 : Current running, BER 0
 Controller T1 2 Profile 2 : Passed with a BER of 0
 Controller T1 3 Profile default : Test Never Ran
 Controller T1 3 Profile 2 : Test Never Ran
 Controller T1 4 Profile default : Test Never Ran
 Controller T1 4 Profile 2 : Test Never Ran
 Controller T1 5 Profile default : Test Never Ran
```

```
 Controller T1 5 Profile 2 : Test Never Ran
 Controller T1 6 Profile default : Test Never Ran
 Controller T1 6 Profile 2 : Test Never Ran
 Controller T1 7 Profile default : Test Never Ran

Controller T1 7 Profile 2 : Test Never Ran
```

The following example shows how the output display was limited to that of only one T1 port, port 0.

```
Router#
show controllers t1 0 bert
Controller T1 0 Profile default : The Test was aborted by User
Controller T1 0 Profile 2 : Test Never Ran
```

show controllers T1-E1 errors

To show the last nineteen alarms on a controller, use the **showcontrollers**command in privileged EXEC mode.

show controllers {**t1** | **e1**} *slot subslot port* **errors**

Syntax Description

slot	Chassis slot number. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide.
subslot	Secondary slot number on a SPA interface processor (SIP) where a SPA is installed. Refer to the platform-specific SPA hardware installation guide and the corresponding "Specifying the Interface Address on a SPA" topic in the platform-specific SPA software configuration guide for subslot information.
port	Interface number on a SPA.
t1	Clear-channel T1 with integrated data service units (DSUs).
e1	Clear-channel E1 with integrated data service units (DSUs).

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(18)SXE	This command was introduced in Cisco IOS Release 12.2(18)SXE to support SPAs on the Cisco 7600 series router and Catalyst 6500 series switch.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **showcontrollers**command to show the last nineteen alarms on a controller on a 8-Port T1/E1 SPA.

Examples

The following example displays the alarms on an E1 interface.

```
Router# #show controllers e1 10/2/4 errors
  E1 10/2/4:Alarm Log Information
  present alarm:NONE
  Alarm:OOF 03:54:17 - 03:54:22
  Alarm:OOF 03:53:34 - 03:54:07
```

Related Commands

Command	Description
controller	Configures a T1, E1, or T3 controller and enters controller configuration mode.
show controller	Displays controller configuration.

show controllers t3

To display information about T3 links and to display hardware and software driver information for the T3 controller, use the **showcontrollerst3**command in privileged EXEC mode.

Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3660 Series, Cisco 3725, and Cisco 3745 Routers
show controllers t3 *slot/port* [{**brief** | **tabular**}]

Cisco 7200 Series Routers
show controllers t3 [*bay/port* [*/t1-channel*]] [{**brief** | **errors** | **tabular** | **remote performance** [{**brief** | **tabular**}]}]

Cisco 7500 Series Routers
show controllers t3 [*slot/bay/port* [*/t1-channel*]] [{**brief** | **errors** | **tabular** | **remote performance** [{**brief** | **tabular**}]}]

Cisco AS5800 Access Servers and Cisco 10000 Series Routers
show controllers t3 *dial-shelf/slot/t3-port*

Cisco Series
show controllers t3 [*slot/bay/port*]

Cisco Series
show controllers t3 [*slot/bay/port path*]

Note This is applicable to 48-Port T3/E3 CEM Interface Module and 1 port OC-48/STM-16 or 4 port OC-12/OC-3 / STM-1/STM-4 + 12 port T1/E1 + 4 port T3/E3 CEM Interface Module.

Syntax Description

slot	Slot number. Refer to the appropriate hardware manual for slot information.
/ *port*	Port number. Refer to the appropriate hardware manual for port information.
slot / *bay* / *port*	Slot number, interface module number in which the slot is inserted, and port number (Cisco series routers).
/ *bay*	(Optional) The port adaptor bay number. Refer to the appropriate hardware manual for bay information
/ *t1-channel*	(Optional) Number from 1 to 28 that represents the T1 channel for the Channelized T3 Interface Processor (CT3IP) on Cisco 7200 series and Cisco 5200 series routers.
dial-shelf	Dial shelf chassis in the Cisco AS5800 access server that contains the CT3 interface card.
/ *slot*	Location of the CT3 interface card in the dial shelf chassis.
/ *t3-port*	T3 port number.

brief	(Optional) Displays a subset of information.
errors	(Optional) Displays a history of alarm events that causes a T3 controller or a T1 controller of a T3 to transition from an Up state to a Down state. The history size is 18 events.
tabular	(Optional) Displays information in a tabular format.
remote performance	(Optional) Displays the far-end ANSI performance monitor information when enabled on the T1 channel with the **t1fdlansi** controller configuration command.
path	Defines the path (sts-1/vc3) information to which the DS3 (T3 or E3) is mapped.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3	This command was introduced.
12.0(3)T	This command was implemented on the Cisco AS5800 access server.
12.2(11)YT	This command was integrated into Cisco IOS Release 12.2(11)YT and implemented on the following platforms: Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3660 series, Cisco 3725, and Cisco 3745 routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(19c)	This command was modified to display error throttling and alarm conditions that cause the T3 controller to enter a failure state.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(31)SB	This command was integrated in Cisco IOS Release 12.2(31)SB.
12.2(33)SB	This command's behavior was modified on the Cisco 10000 series router for the PRE3 and PRE4.
XE Everest 16.5.1	This command was implemented on the Cisco ASR 900 Series Routers and Cisco NCS 4200 Series.
XE Fuji 16.8.x	This command output was modified on the Cisco Series Routers to display far-end counters for performance monitoring.
XE Fuji 16.8.x	The path keyword is introduced in Cisco IOS XE Fuji 16.8.x release for Cisco ASR 900 Series Routers and Cisco NCS 4200 Series Routers for 48-Port T3/E3 CEM Interface Module and 1 port OC-48/STM-16 or 4 port OC-12/OC-3 / STM-1/STM-4 + 12 port T1/E1 + 4 port T3/E3 CEM Interface Module.

Usage Guidelines

Cisco 7500 Series Routers

This command displays controller status that is specific to the controller hardware. The information displayed is generally useful for diagnostic tasks performed by technical support personnel only.

When you use the errors keyword, this command displays history that identifies which alarm events caused a T3 or T1 controller of a T3 to go down for the Cisco 7500 and Cisco 7200 series routers.

Note T1 channels on the CT3IP are numbered 1 to 28 rather than the more traditional zero-based numbering scheme (0 to 27) used with other Cisco products. This is to ensure consistency with telco numbering schemes for T1 channels within channelized T3 equipment.

The **showcontrollerst3**command also displays Maintenance Data Link (MDL) information (received strings) if MDL is configured and framing is set to C-bit.

Cisco 10000 Series Router Usage Guidelines

In releases prior to Cisco IOS Release 12.2(33)SB, when you configure the t1 loopback remote command on the local router, the command also displays in the running configuration file of the far-end router. This is due to the Route Processor (RP) updating an incorrect parameter when it receives the loopback event message from the line card for loopback requests from the far end.

In Cisco IOS Release 12.2(33)SB, the RP updates the correct parameter and the show controllers command correctly displays the loopback CLI commands applied on the local end and displays the loopback events and status received from the line card in response to loopback requests from the far end.

This change in behavior affects the following line cards and is documented in the CSCsm84447 caveat:

- 4-port channelized STM1
- 1-port channelized OC-12
- 6-port channelized T3
- 4-port half-height channelized T3

In Cisco IOS Release 12.2(33)SB, the output from the show controller command includes line code information for the 6-port channelized T3 line card and the 8-port E3/DS3 line card. However, because SONET line cards do not have a direct physical link at the T3 or E3 level, the output from the show controller t3 command does not include line code information.

In Cisco IOS Release 12.2(31)SB, the output from the show controller command displays line code information. The output of the show controller t3 command for SONET-based T3 also includes line code information.

Examples

Cisco 7200 Series Routers

The following is partial output from the **showcontrollerst3** errors command for Cisco IOS Release 12.2(19c) for a specific T1 controller of a T3 on a Cisco 7200 series router with a bay/port of 4/1, displaying the T1 1 alarm event of OOF:

```
Router# show controllers t3 4/1/1 errors
  T3 4/1: Error Log Information
  present alarm: NONE
  Error: AIS
  17:28:08-17:29:18
  T1 1 Error Log Information
```

```
  present alarm: OOF
  Since 17:30:55
  Error: OOF
  17:30:09-17:30:46
```

The following is partial output from the **showcontrollerst3** errors command from Cisco IOS Release 12.2(19c) for a T3 controller on a Cisco 7200 series router with a bay/port of 4/1, displaying a history of all alarm events on all 28 T1 channels:

```
Router# show controllers t3 4/1 errors
  T3 4/1: Error Log Information
  present alarm: NONE
  Error: AIS
  17:28:08-17:29:18
  T1 1 Error Log Information
  present alarm: OOF
  Since 17:30:55
  Error: OOF
  17:30:09-17:30:46
  T1 2 Error Log Information
  present alarm: NONE
  T1 3 Error Log Information
  present alarm: NONE
  T1 4 Error Log Information
  present alarm: NONE
  T1 5 Error Log Information
  present alarm: NONE
  T1 6 Error Log Information
  present alarm: NONE
  T1 7 Error Log Information
  present alarm: NONE
  T1 8 Error Log Information
  present alarm: NONE
  T1 9 Error Log Information
  present alarm: NONE
  T1 10 Error Log Information
  present alarm: NONE
  T1 11 Error Log Information
  present alarm: NONE
 .
 .
 .
```

.Cisco 7500 Series Routers

The following is partial output from the **showcontrollerst3** errors command from Cisco IOS Release 12.2(19c) for a T3 controller with a slot/bay/port of 1/4/1, displaying a history of all alarm events on all 28 T1 channels:

```
Router# show controllers t3 1/4/1 errors
  T3 1/4/1: Error Log Information
  present alarm: NONE
  Error: AIS
  17:28:08-17:29:18
  T1 1 Error Log Information
  present alarm: OOF
  Since 17:30:55
  Error: OOF
  17:30:09-17:30:46
  T1 2 Error Log Information
```

```
  present alarm: NONE
  T1 3 Error Log Information
  present alarm: NONE
  T1 4 Error Log Information
  present alarm: NONE
  T1 5 Error Log Information
  present alarm: NONE
  T1 6 Error Log Information
  present alarm: NONE
  T1 7 Error Log Information
  present alarm: NONE
.
.
.
```

The following is partial output from the **showcontrollerst3** errors command from Cisco IOS Release 12.2(19c) for a specific T1 controller of a T3 on a Cisco 7200 series router with a bay/port of 4/1, displaying the T1 1 alarm event of OOF:

```
Router# show controllers t3 4/1/1 errors
  T3 4/1: Error Log Information
  present alarm: NONE
  Error: AIS
  17:28:08-17:29:18
  T1 1 Error Log Information
  present alarm: OOF
  Since 17:30:55
  Error: OOF
  17:30:09-17:30:46
.
.
.
```

The table below describes the error field shown in the display.

*Table 85: **show controllers t3** Error Field Description*

Field	Description
AIS	alarm indication signal. In a T1 transmission, an all-ones signal transmitted in lieu of the normal signal to maintain transmission continuity and to indicate to the receiving terminal that there is a transmission fault that is located either at, or upstream from, the transmitting terminal.
RAI	remote alarm indication. Indicates a yellow alarm from the remote end of the T1 transmission.
OOF	out of frame. An OOF defect is detected when any three or more errors in sixteen or fewer consecutive F-bits occur.
LOS	loss of signal. A loss of signal occurs when n consecutive zeros is detected on an incoming signal.
NONE	No error is detected.

The following is partial output from the **showcontrollerst3** command from Cisco IOS Release 12.2(19c):

```
Router# show controllers t3 2/1/0
T3 2/1/0 is down.  Hardware is 2CT3 single wide port adapter
  CT3 H/W Version:0.2.2, CT3 ROM Version:1.0, CT3 F/W Version:2.5.1
  FREEDM version:1, reset 0 resurrect 0
```

```
  Applique type is Channelized T3
  Transmitter is sending remote alarm.
  Receiver has loss of signal.
  FEAC code received:No code is being received
  Framing is M23, Line Code is B3ZS, Clock Source is Internal
  Rx-error throttling on T1's ENABLED
  Rx throttle total 0, equipment customer loopback
  Data in current interval (545 seconds elapsed):
     0 Line Code Violations, 0 P-bit Coding Violation
     0 C-bit Coding Violation, 0 P-bit Err Secs
     0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
     545 Unavailable Secs, 0 Line Errored Secs
     0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
  Data in Interval 1:
     0 Line Code Violations, 0 P-bit Coding Violation
     0 C-bit Coding Violation, 0 P-bit Err Secs
     0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
     900 Unavailable Secs, 0 Line Errored Secs
     0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
  Data in Interval 2:
<snip>
```

The following is partial output from the **showcontrollerst3** command from Cisco IOS Release 12.2(19c) for the T1 channel of the T3 controller:

```
Router# show controllers t3 2/1/0
T3 2/1/0 is down.  Hardware is 2CT3 single wide port adapter
  CT3 H/W Version:0.2.2, CT3 ROM Version:1.0, CT3 F/W Version:2.5.1
  FREEDM version:1, reset 0 resurrect 0

  T1 1 is down
  timeslots:1-24
  FDL per AT&T 54016 spec.
  Receiver has loss of signal.
  Framing is ESF, Clock Source is Internal
  Data in current interval (0 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
     0 Unavail Secs, 0 Stuffed Secs
```

The following is partial output from the **showcontrollerst3** command:

```
Router# show controllers t3 3/0/0
T3 3/0/0 is up.
  CT3 H/W Version: 4, CT3 ROM Version: 0.116, CT3 F/W Version: 0.10.0
  Mx H/W version: 2, Mx ucode ver: 1.24
  Applique type is Channelized T3
  No alarms detected.
  FEAC code received: No code is being received
  Framing is M23, Line Code is B3ZS, Clock Source is Internal.
  Ext1: LOS, Ext2: LOS, Ext3: LOS, Test: OK
  Data in current interval (39 seconds elapsed):
     0 Line Code Violations, 0 P-bit Coding Violation
     0 C-bit Coding Violation
     0 P-bit Err Secs, 0 P-bit Severely Err Secs
     0 Severely Err Framing Secs, 0 Unavailable Secs
     0 Line Errored Secs, 0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
  Total Data (last 1 15 minute intervals):
     0 Line Code Violations, 0 P-bit Coding Violation,
     0 C-bit Coding Violation,
     0 P-bit Err Secs, 0 P-bit Severely Err Secs,
```

```
     0 Severely Err Framing Secs, 0 Unavailable Secs,
     0 Line Errored Secs, 0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
.
.
.
T1 1 is down, speed: 1536 kbs, non-inverted data
  timeslots: 1-24
  FDL per ANSI T1.403 and AT&T 54016 spec.
  Configured for FDL Remotely Line Looped
  No alarms detected.
  Framing is ESF, LineCode is B8ZS, Clock Source is Internal.
  BERT test result (running)
      Test Pattern: All 0's, Status: Sync, Sync Detected: 1
      Interval: 4 minute(s), Tim Remain: 4 minute(s)
      Bit Errors (Sync BERT Started): 0 bits
      Bit Errors (Sync last Sync): 0 bits, Bits Received: 7 Mbits
```

The following is partial output from the **showcontrollerst3brief** command:

```
Router# show controllers t3 3/0/0 brief
T3 3/0/0 is up.
  CT3 H/W Version: 4, CT3 ROM Version: 0.116, CT3 F/W Version: 0.10.0
  Mxt H/W version: 2, Mxt ucode ver: 1.24
  Applique type is Channelized T3
  No alarms detected.
  FEAC code received: No code is being received
  Framing is M23, Line Code is B3ZS, Clock Source is Internal.
  Ext1: LOS, Ext2: LOS, Ext3: LOS, Test: OK
  T1 1 is up, speed: 1536 kbs, non-inverted data
  timeslots: 1-24
  FDL per ANSI T1.403 and AT&T 54016 spec.
  Configured for FDL Remotely Line Looped
  No alarms detected.
  Framing is ESF, LineCode is B8ZS, Clock Source is Internal.
  BERT test result (done)
      Test Pattern: All 0's, Status: Not Sync, Sync Detected: 1
      Interval: 4 minute(s), Tim Remain: 0 minute(s)
      Bit Errors(Sync BERT Started): 0 bits
      Bit Errors(Sync last Sync): 0 bits, Bits Received: 368 Mbits
.
.
.
```

The following is partial output from the **showcontrollerst3tabular** command:

```
Router# show controllers t3 3/0/0 tabular

T3 3/0/0 is up.
  CT3 H/W Version: 4, CT3 ROM Version: 1.2, CT3 F/W Version: 2.1.0
  Mx H/W version: 2, Mx ucode ver: 1.25
  Applique type is Channelized T3
  No alarms detected.
  MDL transmission is disabled

  FEAC code received: No code is being received
  Framing is C-BIT Parity, Line Code is B3ZS, Clock Source is Internal.
  Ext1: AIS, Ext2: LOS, Ext3: LOS, Test: LOS
  INTERVAL      LCV   PCV   CCV   PES  PSES  SEFS   UAS   LES   CES  CSES
  08:56-09:11     0     0     0     0     0     0     0     0     0     0
  08:41-08:56     0     0     0     0     0     0     0     0     0     0
  08:26-08:41     0     0     0     0     0     0     0     0     0     0
  Total           0     0     0     0     0     0     0     0     0     0
.
```

```
.
.
T1 2 is up, speed: 1536 kbs, non-inverted data
  timeslots: 1-24
  FDL per AT&T 54016 spec.
  No alarms detected.
  Framing is ESF, Line Code is B8ZS, Clock Source is Internal.
  INTERVAL      LCV   PCV   CSS  SELS   LES    DM    ES   BES   SES   UAS    SS
  08:56-09:11     0     0     0     0     0     0     0     0     0     0     0
  08:41-08:56     0     0     0     0     0     0     0     0     0     0     0
  08:26-08:41     0     0     0     0     0     0     0     0     0     0     0
  Total           0     0     0     0     0     0     0     0     0     0     0
```

The following output shows a controller with a high number of errors on the line, thus showing a throttle count (RX throttles).

```
Router# show controllers t3 6/0/0 tabular
  T1 2 is up
  timeslots: 1-24
  FDL per AT&T 54016 spec.
  No alarms detected.
  Framing is ESF, Clock Source is Line, Rx throttles 47
  INTERVAL      LCV   PCV   CSS  SELS   LES    DM    ES   BES   SES   UAS SS
  07:48-07:53     0     0     0     0     0     0     0     0     0     0
```

The following is partial output from the **showcontrollerst3remoteperformance** command. This information is available if the**t1fdlansi** controller configuration command is enabled for a T1 channel on a CT3IP.

```
Router# show controllers t3 3/0/0 remote performance
T3 3/0/0 is up.
  CT3 H/W Version: 4, CT3 ROM Version: 0.116, CT3 F/W Version: 20.2.0
  Mx H/W version: 2, Mx ucode ver: 1.25
  T1 1 - Remote Performance Data
  Data in current interval (356 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
     0 Unavail Secs
  Data in Interval 1:
     1 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     2 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
     0 Unavail Secs
  Data in Interval 2:
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
     0 Unavail Secs
  Total Data (last 2 15 minute intervals):
     1 Path Code Violations
     1 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins,
     2 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
     0 Unavail Secs
.
.
.
```

The table below describes the fields shown in the display.

*Table 86: **show controllers t3** Field Descriptions--Cisco 7500 Series*

Field	Description
T3 3/0/0 is up	T3 controller in slot 3 is operating. The controller's state can be up, down, or administratively down. Loopback conditions are shown by (Locally Looped) or (Remotely Looped).
CT3 H/W Version	Version number of the hardware.
CT3 ROM Version	Version number of the ROM.
CT3 F/W Version	Version number of the firmware.
Mx H/W version	Hardware version number of the HDLC controller chip.
Mx ucode ver	Microcode version of the HDLC controller chip.
Applique type	Controller type.
No alarms detected	Any alarms detected by the controller are displayed here. Possible alarms are as follows: • Transmitter is sending remote alarm. • Transmitter is sending AIS. • Receiver has loss of signal. • Receiver is getting AIS. • Receiver has loss of frame. • Receiver has remote alarm. • Receiver has no alarms.
MDL transmission	Status of the Maintenance Data Link (either enabled or disabled).

Field	Description
FEAC code received	Whether or not a far-end alarm code request is being received. Possible values are as follows: • DS3 Eqpt. Failure (SA) • DS3 LOS/HBER • DS3 Out-of-Frame • DS3 AIS Received • DS3 IDLE Received • DS3 Eqpt. Failure (NSA) • Common Eqpt. Failure (NSA) • Multiple DS1 LOS/HBER • DS1 Eqpt. Failure • Single DS1 LOS/HBER • DS1 Eqpt. Failure (NSA) • No code is being received
Framing	Framing type on the CT3IP. Values are M23, C-Bit, and Auto-detect.
Line Code	Line coding format on the CT3IP.
Clock Source	Clock source on the CT3IP. Values are internal or line.
RX-error throttling	Indicates that error throttling is enabled. The error throttling command disables the T1 level clock in order to stop receiving error data packets on a T1 controller. If any single interface receives a burst of errors over a short duration, such as 400 errors in 100 milliseconds, the T1 clock will be turned off for a period of 100 milliseconds.
RX throttles	The presence of the throttle count indicates that there are many input errors on lines. On the CT3 PA, the T1 is throttled when there are a number of input errors on an interface (400 errors in 100 milliseconds). The T1 is throttled even if one of the interfaces on it sees continuous errors. The 1-second periodic process checks for throttled interfaces and unthrottles them back.

Field	Description
BERT test result	BERT test information is available if the **t1bert** controller configuration command is enabled for the T1 channel on the CT3IP. The BERT results include the following information: • Test Pattern--Type of test pattern selected. • Status--Status of the test. • Sync Detected--Number of times the pattern synch is detected (that is, the number of times the pattern goes from No Sync to Sync). • Interval--Duration selected. • Tim Remain--Time remaining on the BERT test. • Bit Errors (Sync BERT Started)--Number of bit errors during the BERT test. • Bit Errors (Sync last Sync)--Number of bit errors since the last pattern sync was detected. • Bits Received--Total bits received. When the T1 channel has a BERT test running, the line state is DOWN. Also, when the BERT test is running and the Status field is Not Sync, the information in the total bit errors field is not valid. When the BERT test is done, the Status field is not relevant.
Data in current interval (39 seconds elapsed)	Shows the current accumulation period, which rolls into the 24-hour accumulation every 15 minutes. Accumulation period is from 1 to 900 seconds. The oldest 15-minute period falls off the back of the 24-hour accumulation buffer.
Line Code Violations	Line Code Violations (LCVs) is a count of both Bipolar Violations (BPVs) and Excessive Zeros (EXZs) that occur over the accumulation period. An EXZ increments the LCV by one regardless of the length of the zero string.
P-bit Coding Violation	For all DS3 applications, a P-bit coding violation (PCV) error event is a P-bit parity error event. A P-bit parity error event is the occurrence of a received P-bit code on the DS3 M-frame that is not identical to the corresponding locally calculated code.
C-bit Coding Violation	For C-bit parity and SYNTRAN DS3 applications, the C-bit coding violation (CCV) is the count of coding violations reported via the C-bits. For C-bit parity, it is the count of CP-bit parity errors that occur during the accumulation interval. For SYNTRAN, it is a count of CRC-9 errors that occur during the accumulation interval.
P-bit Err Secs	P-bit errored seconds (PES) is a second with one or more PCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when unavailable seconds are counted.

Field	Description
P-bit Severely Err Secs	P-bit severely errored seconds (PSES) is a second with 44 or more PCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when unavailable seconds are counted.
Severely Err Framing Secs	Severely errored framing seconds (SEFS) is a second with one or more out-of-frame defects or a detected incoming AIS.
Unavailable Secs	The number of unavailable seconds (UAS) is calculated by counting the number of seconds for which the interface is unavailable. For more information, refer to RFC 1407, *DS3 MIB Variables* .
Line Errored Secs	Line errored seconds (LES) is a second in which one or more code violations or one or more LOS defects occurred.
C-bit Errored Secs	C-bit errored seconds (CES) is a second with one or more C-bit code violations (CCV), one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when UASs are counted.
C-bit Severely Errored Secs	C-bit severely errored seconds (CSES) is a second with 44 or more CCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when UASs are counted.
Total Data (last 1 15 minute intervals)	Shows the last 15-minute accumulation period.
T1 1 is up	T1 channel is operating. The channel's state can be up, down, or administratively down. Loopback conditions are shown by (Locally Looped) or (Remotely Looped).
speed	Speed of the T1 channel, in kbps.
non-inverted data	Indicates if the T1 channel is configured for inverted data.
timeslots	Time slots assigned to the T1 channel.
FDL per ANSI T1.403 and AT&T 54016 spec.	Performance monitoring is via Facility Data Link per ANSI T1.403 and AT&T standard specification number 54016.
No alarms detected	Any alarms detected by the T1 controller are displayed here. Possible alarms are as follows: • Transmitter is sending remote alarm. • Transmitter is sending AIS. • Receiver has loss of signal. • Receiver is getting AIS. • Receiver has loss of frame. • Receiver has remote alarm. • Receiver has no alarms.

Field	Description
Framing	Type of framing used on the T1 channel. Values are ESF or SF.
Line Code	Type of line coding used on the T1 channel. Values are B8ZS or AMI.
Clock Source	Clock source on the T1 channel. Values are internal or line.
Path Code Violations	Path coding violation (PCV) error event is a frame synchronization bit error in the D4 and E1-no-CRC formats or a CRC error in the ESF and E1-CRC formats.
Slip Secs	Controlled slip second (CSS) is a 1-second interval that contains one or more controlled slips.
Fr Loss Secs	Frame loss seconds (SELS) is the number of seconds for which an out-of-frame error is detected.
Line Err Secs	Line errored seconds (LES) is a second in which one or more line code violation errors are detected.
Degraded Mins	Degraded minute (DM) is a minute in which the estimated error rate exceeds 1E-6 but does not exceed 1E-3. For more information, refer to RFC 1406, *Definitions of Managed Objects for DS1 and E1 Interface Types* .
Errored Secs	Errored seconds (ES) is a second with one or more path coding violations, one or more out-of-frame defects, or one or more controlled slip events or a detected AIS defect.
Bursty Err Secs	Bursty errored seconds (BES) is a second with fewer than 320 and more than one path coding violation error events, no severely errored frame defects, and no detected incoming AIS defects. Controlled slips are not included in this parameter.
Severely Err Secs	Severely errored seconds (SES) is a second with 320 or more path code violation errors events, one or more out-of-frame defects, or a detected AIS defect.
Unavailable Secs	Number of seconds during which the interface was not available in this interval. Referred to as UAS.
Stuffed Secs	Stuffed seconds (SS) is a second in which one more bit stuffings take place. This happens when the Pulse Density Enforcer detects a potential violation in the output stream and inserts a 1 to prevent it. Such bit stuffings corrupt user data and indicate that the network is configured incorrectly. This counter can be used to help diagnose this situation.

Cisco AS5800 Access Servers

The following example shows the summary status of the T3 controller located in shelf 1, slot 4, port 0:

```
Router# show controllers t3 1/4/0 brief
T3 1/4/0 is up.
 Applique type is Channelized T3
```

```
 No alarms detected.
 MDL transmission is disabled

 FEAC code received: Multiple DS1 LOS/HBER
 Framing is C-BIT Parity, Line Code is B3ZS, Clock Source is Line.
 Data in current interval (491 seconds elapsed):
     0 Line Code Violations, 0 P-bit Coding Violation
     0 C-bit Coding Violation, 0 P-bit Err Secs
     0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
     0 Unavailable Secs, 0 Line Errored Secs
     0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
 Total Data (last 80 15 minute intervals):
     3 Line Code Violations, 4 P-bit Coding Violation,
     2 C-bit Coding Violation, 0 P-bit Err Secs,
     0 P-bit Severely Err Secs, 0 Severely Err Framing Secs,
     2 Unavailable Secs, 0 Line Errored Secs,
     0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
```

The following example shows the detailed status of the T3 controller connected to the Cisco AS5800 in shelf 1, slot 4, port 0. Notice that the detailed information shows the last eighty-six 15-minute time periods.

```
Router# show controllers t3 1/4/0
T3 1/4/0 is up.
 Applique type is Channelized T3
 No alarms detected.
 MDL transmission is disabled

 FEAC code received: Multiple DS1 LOS/HBER
 Framing is C-BIT Parity, Line Code is B3ZS, Clock Source is Line.
 Data in current interval (91 seconds elapsed):
     0 Line Code Violations, 0 P-bit Coding Violation
     0 C-bit Coding Violation, 0 P-bit Err Secs
     0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
     0 Unavailable Secs, 0 Line Errored Secs
     0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
 Data in Interval 1:
     0 Line Code Violations, 0 P-bit Coding Violation
     0 C-bit Coding Violation, 0 P-bit Err Secs
     0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
     0 Unavailable Secs, 0 Line Errored Secs
     0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
 Data in Interval 2:
     0 Line Code Violations, 0 P-bit Coding Violation
     0 C-bit Coding Violation, 0 P-bit Err Secs
     0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
     0 Unavailable Secs, 0 Line Errored Secs
     0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
 Data in Interval 3:
     0 Line Code Violations, 0 P-bit Coding Violation
     0 C-bit Coding Violation, 0 P-bit Err Secs
     0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
     0 Unavailable Secs, 0 Line Errored Secs
     0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
 Data in Interval 4:
     0 Line Code Violations, 0 P-bit Coding Violation
     0 C-bit Coding Violation, 0 P-bit Err Secs
     0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
     0 Unavailable Secs, 0 Line Errored Secs
     0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
.
.
.
```

```
Data in Interval 86:
     3 Line Code Violations, 4 P-bit Coding Violation
     2 C-bit Coding Violation, 0 P-bit Err Secs
     0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
     2 Unavailable Secs, 0 Line Errored Secs
     0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
 Total Data (last 86 15 minute intervals):
     3 Line Code Violations, 4 P-bit Coding Violation,
     2 C-bit Coding Violation, 0 P-bit Err Secs,
     0 P-bit Severely Err Secs, 0 Severely Err Framing Secs,
     2 Unavailable Secs, 0 Line Errored Secs,
     0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
```

The table below describes the fields shown in the display.

Table 87: show controllers t3 Field Descriptions--Cisco AS5800

Field	Description
T3 1/4/0 is up	T3 controller connected to this Cisco AS5800 access server in shelf 1, slot 4, port 0 is up. The controller's state can be up, down, or administratively down. Loopback conditions are shown by Locally Looped or Remotely Looped.
Applique type	Describes the type of controller.
No alarms detected	Any alarms detected by the controller are displayed here. Possible alarms are as follows: • Transmitter is sending remote alarm. • Transmitter is sending alarm indication signal (AIS). • Receiver has loss of signal (LOS). • Receiver is getting AIS. • Receiver has loss of frame (LOF). • Receiver has remote alarm. • Receiver has no alarms.
MDL transmission	Maintenance Data Link status (either enabled or disabled). Used for carrying performance information and control signals across the network toward the far-end T3 unit. It is the counterpart of Facility Data Link (FDL) in a T1 link.

Field	Description
FEAC code received	Whether or not a far-end alarm code request is being received. Possible values are as follows: • DS3 Eqpt. Failure (SA) • DS3 LOS/HBER • DS3 Out-of-Frame • DS3 AIS Received • DS3 IDLE Received • DS3 Eqpt. Failure (NSA) • Common Eqpt. Failure (NSA) • Multiple DS1 LOS/HBER • DS1 Eqpt. Failure • Single DS1 LOS/HBER • DS1 Eqpt. Failure (NSA) • No code is being received
Framing	Standard T3 framing type: M23, C-Bit, or Auto-detect.
Line Code	Standard T3 line-coding format. In this example, the line-coding format is bipolar 3-zero substitution (B3ZS).
Clock Source	The source of the synchronization signal (clock): line or internal. In this example, the line is providing the clock signal.
Data in current interval (... seconds elapsed)	Summary statistics for T3 signal quality for the current time interval of 900 seconds (15 minutes). In this example, the statistics are for current partial interval. Statistics roll into the 24-hour accumulation buffer every 15 minutes. The oldest 15-minute period falls off the back of the 24-hour accumulation buffer.
Line Code Violations	Count of both Bipolar Violations (BPVs) and Excessive Zeros (EXZs) that occur over the accumulation period. An EXZ increments the Line Code Violations (LCVs) by one regardless of the length of the zero string.
P-bit Coding Violation	P-bit parity error event. A P-bit parity error event is the occurrence of a received P-bit code on the DS3 M-frame that is not identical to the corresponding locally calculated code. Referred to as PCV.
C-bit Coding Violation	Count of coding violations reported via the C-bits. For C-bit parity, it is the count of CP-bit parity errors that occur during the accumulation interval. Referred to as CCV.

Field	Description
P-bit Err Secs	Number of seconds with one or more PCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when unavailable seconds are counted.
P-bit Severely Err Secs	Number of seconds with 44 or more PCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when unavailable seconds are counted.
Severely Err Framing Secs	Number of a seconds with one or more out-of-frame defects or a detected incoming AIS.
Unavailable Secs	Number of seconds during which the interface was not available in this interval. Referred to as UAS.
Line Errored Secs	Number of seconds in this interval during which one or more code violations or one or more LOS defects occurred. Referred to as LES.
C-bit Errored Secs	Number of seconds with one or more C-bit code violations (CCV), one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when UASs are counted. Referred to as CES.
C-bit Severely Errored Secs	Number of seconds with 44 or more CCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when UASs are counted.
Total Data (last ... 15 minute intervals)	Summary statistics for T3 signal quality for 15-minute intervals. Every 24 hours (96 intervals) the counters in this data block clear.

Cisco 10000 Series Router Examples

The following examples from the show controller t3 command show the information that displays when the router is running Cisco IOS Release 12.2(33)SB and Cisco IOS Release 12.2(31)SB:

Cisco IOS Release 12.2(33)SB --No Line Code Information (CHSTM1 and 1CHOC12 Cards)

```
Router# show controllers t3 2/0/0.1
T3 2/0/0.1 is up. Hardware is C10K CHSTM1 line card
Applique type is Channelized T3
Controller is in channelized mode
No alarms detected.
MDL transmission is disabled
FEAC code received: No code is being received
Framing is C-BIT Parity (Detected), Clock Source is Internal
equipment customer loopback
Data in current interval (155 seconds elapsed):
290738 P-bit Coding Violation
290736 C-bit Coding Violation, 0 P-bit Err Secs
0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
34 Unavailable Secs, 0 Line Errored Secs
0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
31 AIS Defect Secs, 0 FERF Defect Secs
```

```
1 Near-end path failures, 0 Far-end path failures
0 CP-bit Far-End Unavailable Secs, 107 Far-End Coding Violations
2 Far-End Errored Secs, 1 Far-End Severely Errored Secs
```

Cisco IOS Release 12.2(31)SB --Line Code Information (CHSTM1 and 1CHOC12 Cards)

```
Router# show controllers t3 2/0/0.1
T3 2/0/0.1 is up. Hardware is C10K CHSTM1 line card
Applique type is Channelized T3
Controller is in channelized mode
No alarms detected.
MDL transmission is disabled
FEAC code received: No code is being received
Framing is C-BIT Parity (Detected), Clock Source is Internal
equipment customer loopback
Data in current interval (155 seconds elapsed):
290738 P-bit Coding Violation
290736 C-bit Coding Violation, 0 P-bit Err Secs
0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
34 Unavailable Secs, 0 Line Errored Secs
0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
```

Cisco IOS Release 12.2(33)SB3-- CHSTM1 and 1CHOC12 Cards

```
Router# show controllers t3 2/0/0.1
T3 2/0/0.1 is up.  Hardware is C10K CHSTM1 line card
  Applique type is Channelized T3
  Controller is in channelized mode
  No alarms detected.
  MDL transmission is disabled

  FEAC code received: No code is being received
  Framing is C-BIT Parity (Detected), Clock Source is Internal
  equipment customer loopback
  Data in current interval (155 seconds elapsed):
     290738 P-bit Coding Violation
     290736 C-bit Coding Violation, 0 P-bit Err Secs
     0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
     34 Unavailable Secs, 0 Line Errored Secs
     0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
     31 AIS Defect Secs, 0 FERF Defect Secs
     1 Near-end path failures, 0 Far-end path failures
     0 CP-bit Far-End Unavailable Secs, 107 Far-End Coding Violations
     2 Far-End Errored Secs, 1 Far-End Severely Errored Secs
```

Cisco IOS Release 12.2(33)SB3 --4HHCT3 and 6CHT3 Cards

```
Router# show controllers t3 8/0/0
T3 8/0/0 is down.  Hardware is C10K Half Height CT3 line card
  Applique type is Channelized T3
  Controller is in channelized mode
  Receiver has loss of signal.
  MDL transmission is disabled

  FEAC code received: No code is being received
  Framing is C-BIT Parity (Configured)
```

```
Line Code is B3ZS, Clock Source is Internal
equipment customer loopback
Data in current interval (617 seconds elapsed):
   6120 Line Code Violations, 0 P-bit Coding Violation
   0 C-bit Coding Violation, 0 P-bit Err Secs
   0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
   25 Unavailable Secs, 0 Line Errored Secs
   0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
   0 AIS Defect Secs, 25 LOS Defect Secs
   1 Near-end path failures
   0 Far-end path failures, 0 FERF Defect Secs
   24 CP-bit Far-End Unavailable Secs, 4771 Far-End Coding Violations
   0 Far-End Errored Secs, 0 Far-End Severely Errored Secs
```

The table below describes the significant fields shown in the display.

Table 88: show controllers t3 Field Descriptions--Cisco 10000 series router

Field	Description
AIS	Alarm indication signal.
T3 2/0/0.1 is up	T3 controller connected to this Cisco 10000 series router in shelf 2, slot 0, port 0.1 is up. The controller's state can be up, down, or administratively down. Loopback conditions are shown by Locally Looped or Remotely Looped.
T3 8/0/0 is down	T3 controller connected to this Cisco 10000 series router in shelf 8, slot 0, port 0 is down. The controller's state can be up, down, or administratively down. Loopback conditions are shown by Locally Looped or Remotely Looped.
Applique type	Describes the type of controller.
No alarms detected	Any alarms detected by the controller are displayed here. Possible alarms are as follows: • Receiver has loss of frame (LOF). • Receiver has loss of signal (LOS). • Receiver has no alarms. • Receiver has remote alarm. • Receiver is getting AIS. • Transmitter is sending alarm indication signal (AIS). • Transmitter is sending remote alarm.
MDL transmission	Maintenance Data Link status (either enabled or disabled). Used for carrying performance information and control signals across the network toward the far-end T3 unit. It is the counterpart of Facility Data Link (FDL) in a T1 link.

Field	Description
FEAC code received	Whether a far-end alarm code request is being received. Possible values are as follows: • Common Eqpt. Failure (NSA) • DS1 Eqpt. Failure (NSA) • DS1 Eqpt. Failure • DS3 AIS Received • DS3 Eqpt. Failure (NSA) • DS3 Eqpt. Failure (SA) • DS3 IDLE Received • DS3 LOS/HBER • DS3 Out-of-Frame • Multiple DS1 LOS/HBER • No code is being received • Single DS1 LOS/HBER
Framing	Standard T3 framing type: M23, C-bit, or Auto-detect.
Line Code	Standard T3 line-coding format. In this example, the line-coding format is bipolar 3-zero substitution (B3ZS).
Clock Source	The source of the synchronization signal (clock): Line or Internal. In this example, the line is providing the clock signal.
Data in current interval (617 seconds elapsed)	Summary statistics for T3 signal quality for the current time interval of 900 seconds (15 minutes). In this example, the statistics are for current partial interval. Statistics roll into the 24-hour accumulation buffer every 15 minutes. The oldest 15-minute period falls off the back of the 24-hour accumulation buffer.
Line Code Violations	Count of both Bipolar Violations (BPVs) and Excessive Zeros (EXZs) that occur over the accumulation period. An EXZ increments the line code violations (LCVs) by one, regardless of the length of the zero string.
P-bit Coding Violation	P-bit parity error event. A P-bit parity error event is the occurrence of a received P-bit code on the DS3 M-frame that is not identical to the corresponding locally calculated code. Referred to as PCV.
C-bit Coding Violation	Count of coding violations reported via the C-bits. For C-bit parity, it is the count of CP-bit parity errors that occur during the accumulation interval. Referred to as CCV.
P-bit Err Secs	Number of seconds with one or more PCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when unavailable seconds are counted.

Field	Description
P-bit Severely Err Secs	Number of seconds with 44 or more PCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when unavailable seconds are counted.
Severely Err Framing Secs	Number of a seconds with one or more out-of-frame defects or a detected incoming AIS.
Unavailable Secs	Number of seconds during which the interface was not available in this interval. Referred to as UAS.
Line Errored Secs	Number of seconds in this interval during which one or more code violations or one or more LOS defects occurred. Referred to as LES.
C-bit Errored Secs	Number of seconds with one or more C-bit code violations (CCV), one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when UASs are counted. Referred to as CES.
C-bit Severely Errored Secs	Number of seconds with 44 or more CCVs, one or more out-of-frame defects, or a detected incoming AIS. This gauge is not incremented when UASs are counted.

Series Router

The following is a sample output from the **show controllers t3** command on the Cisco series routers:

```
Router# show controllers t3 0/4/40
T3 0/4/40 is up.
Hardware is -48T3E3-CE
Applique type is Clear Channel T3
No alarms detected.
MDL transmission is disabled
FEAC code received: No code is being received
Framing is C-BIT Parity, Line Code is B3ZS, Cablelength Short less than 225ft
BER thresholds: SF = 10e-10 SD = 10e-10
Clock Source is internal
Equipment customer loopback
Data in current interval (240 seconds elapsed):
  Near End
     0 Line Code Violations, 0 P-bit Coding Violations
     0 C-bit Coding Violations, 0 P-bit Err Secs
     0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
     0 Unavailable Secs, 0 Line Errored Secs
     0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
     0 Severely Errored Line Secs, 0 Path Failures
     0 AIS Defect Secs, 0 LOS Defect Secs
   Far End
     0 Errored Secs, 0 Severely Errored Secs
     0 C-bit Unavailable Secs, 0 Path Failures
     0 Code Violations, 0 Service Affecting Secs
  Data in Interval 1:
   Near End
     0 Line Code Violations, 0 P-bit Coding Violations
     0 C-bit Coding Violations, 0 P-bit Err Secs
     0 P-bit Severely Err Secs, 0 Severely Err Framing Secs
     20 Unavailable Secs, 20 Line Errored Secs
```

```
      0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
      20 Severely Errored Line Secs, 1 Path Failures
      0 AIS Defect Secs, 20 LOS Defect Secs
    Far End
      0 Errored Secs, 0 Severely Errored Secs
      0 C-bit Unavailable Secs, 0 Path Failures
      0 Code Violations, 0 Service Affecting Secs
   Total Data (last 1 15 minute intervals):
    Near End
      0 Line Code Violations, 0 P-bit Coding Violations,
      0 C-bit Coding Violations, 0 P-bit Err Secs,
      0 P-bit Severely Err Secs, 0 Severely Err Framing Secs,
      20 Unavailable Secs, 20 Line Errored Secs,
      0 C-bit Errored Secs, 0 C-bit Severely Errored Secs
      20 Severely Errored Line Secs, 1 path failures
      0 AIS Defect Secs, 20 LOS Defect Secs
    Far End
      0 Errored Secs, 0 Severely Errored Secs
      0 C-bit Unavailable Secs, 0 Path Failures
      0 Code Violations, 0 Service Affecting Secs
 T1 1 is up
   timeslots:
   FDL per AT&T 54016 spec.
   No alarms detected.
   Framing is ESF, Clock Source is Internal
   Data in current interval (250 seconds elapsed):
    Near End
      0 Line Code Violations, 0 Path Code Violations
      0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
      0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
      0 Unavailable Secs, 0 Stuffed Secs
      0 Path Failures, 0 SEF/AIS Secs
    Far End
      0 Line Code Violations, 0 Path Code Violations
      0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
      0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs
      0 Unavailable Secs 0 Path Failures
   Data in Interval 1:
    Near End
      0 Line Code Violations, 0 Path Code Violations
      0 Slip Secs, 2 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
      2 Errored Secs, 0 Bursty Err Secs, 2 Severely Err Secs
      0 Unavailable Secs, 0 Stuffed Secs
      1 Path Failures, 2 SEF/AIS Secs
    Far End
      0 Line Code Violations, 0 Path Code Violations
      0 Slip Secs, 2 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
      3 Errored Secs, 0 Bursty Err Secs, 3 Severely Err Secs
      0 Unavailable Secs 0 Path Failures
   Total Data (last 1 15 minute intervals):
    Near End
      0 Line Code Violations,0 Path Code Violations,
      0 Slip Secs, 2 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins,
      2 Errored Secs, 0 Bursty Err Secs, 2 Severely Err Secs
      0 Unavailable Secs, 0 Stuffed Secs
      1 Path Failures, 2 SEF/AIS Secs
    Far End
      0 Line Code Violations,0 Path Code Violations
      0 Slip Secs, 2 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins,
      3 Errored Secs, 0 Bursty Err Secs, 3 Severely Err Secs
      0 Unavailable Secs, 0 Path Failures
```

Use **show controller t3** *0/1/20 path* to verify DS3 CEP configuration:

```
rtr2#show controller t3 0/1/20 path

T3 0/1/20 PATH 1.

Asynchronous Mapping for DS3 into STS-1

TX : TDM to PSN direction
RX : PSN to TDM direction

Clock Source is internal

  AIS = 0          RDI = 0          REI = 349        BIP(B3) = 22
  LOP = 0          PSE = 0          NSE = 0          NEWPTR = 0
  LOM = 0          PLM = 0          UNEQ = 0
Active Defects: None
Detected Alarms: None
Asserted/Active Alarms: None
Alarm reporting enabled for: None

TCA threshold:  B3 = 10e-6
Rx: C2 = FF
Tx: C2 = 01

Tx J1 Length : 64
Tx J1 Trace

  72 74 72 32 20 30 2F 31 2F 32 30 2E 31 00 00 00     rtr2 0/1/20.1...
  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00     ................
  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00     ................
  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00     ................

Expected J1 Length : 64
Expected J1 Trace

  72 74 72 32 20 30 2F 31 2F 32 30 2E 31 00 00 00     rtr2 0/1/20.1...
  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00     ................
  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00     ................
  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00     ................

PATH TRACE BUFFER : UNSTABLE

Rx J1 Length : 64
Rx J1 Trace

  72 73 70 32 20 30 2F 35 2F 31 32 2E 31 00 00 00     rsp2 0/5/12.1...
  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00     ................
  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00     ................
  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00     ................

rtr2#
```

Note The verification output does not provide the alarm details.

show controllers t3 bert

To display BER test statistics, use the show controllers t3 bert command in user EXEC or privileged EXEC mode.

show controllers t3 *slot/subslot/port* [/*t1-number*] **bert**

Syntax Description

slot	Chassis line card slot number.
subslot	Chassis line card subslot number.
port	Interface number on the line card.
t1-number	(Optional) Logical T1 interface number.
bert	Displays BER test statistics.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced on the Cisco 10000 series routers.

Examples

The following example shows BER test statistics for an unchannelized T3 interface:

```
Router# show controllers t3 6/1/0 bert

T3 6/1/0 is up.
BERT test result (done)
Test Pattern : 2^15, Status : Not Sync, Sync Detected : 1
Interval : 5 minute(s), Time Remain : 0 minute(s)
Bit Errors (since BERT started): 0 bits,
Bits Received (since BERT started): 13025 Mbits
Bit Errors (since last sync): 0 bits
Bits Received (since last sync): 13025 Mbits
```

The following example shows BER test statistics for a channelized T3 interface:

```
Router# show controllers t3 6/1/0 bert

T3 6/1/0 is up.
BERT test result (running)
Test Pattern : 2^15, Status : Sync, Sync Detected : 1
Interval : 3 minute(s), Time Remain : 1 minute(s)
Bit Errors (since BERT started): 0 bits,
Bits Received (since BERT started): 5493 Mbits
Bit Errors (since last sync): 0 bits
Bits Received (since last sync): 5493 Mbits
```

The following example shows BER test statistics for a T1 interface:

```
Router# show controllers t3 6/1/1/1 bert

T3 6/1/1/1 is up. Hardware is C10K Half Height CT3 line card
T1 1
BERT test result (running)
Test Pattern : 2^15, Status : Sync, Sync Detected : 1
Interval : 5 minute(s), Time Remain : 5 minute(s)
Bit Errors (since BERT started): 0 bits,
Bits Received (since BERT started): 36 Mbits
Bit Errors (since last sync): 0 bits
Bits Received (since last sync): 36 Mbits
```

Related Commands

Command	Description
bert	Configures a BER test for an unchannelized or channelized T3 interface.
t1 bert pattern	Configures a BER test for a T1 interface.

show controllers token

To display information about memory management and error counters on the Token Ring Interface Processor (TRIP) for the Cisco 7500 series routers, use the **showcontrollerstoken** command in privileged EXEC mode.

show controllers token

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
11.3(3)T	The information was modified to include the PA-4R-FDX full-duplex Token Ring port adapter.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Depending on the card being used, the output can vary. This command also displays information that is proprietary to Cisco Systems. Thus, the information that the **showcontrollerstoken** command displays is of primary use to Cisco technical personnel. Information that is useful to users can be obtained with the **showinterfacestokenring** command, which is described later in this chapter.

Examples

The following is sample output for the PA-4R-DTR from the **showcontrollerstoken**command. In this example, the current operating mode is classic Token Ring station.

```
Router# show controllers token
Interface TokenRing4/0 state: up
  Data from IDB:
    Current MAC address: 0008.2a36.1a04, Burned in MAC address: 0008.2a36.1a04
    Group address: 80000000
    Functional address: 08000000, enables: CDP
    Ring mode: 0000, enables:
  Last Ring Status: none
    Stats: soft: 0/0, hard: 0/0, sig loss: 0/0, throttle: 0/0
           tx beacon: 0/0, wire fault 0/0, recovery: 0/0
           only station: 0/0, remote removal: 0/0
  Interface failures: 0
  Current operating mode:
    Classic token ring station
      MAC state: inserted
      Duplex: half
      Access protocol: TKP
      Ring speed: 16 Mbps
      Ring monitor role: Standby monitor
  Internal controller data:
    MAC microcode version: 0.240
    Hawkeye ASIC revision: 0
    Node address: 0008.2a36.1a04
    Functional address: 08000000, Group address: 80000000
```

```
Hawkeye ASIC registers:
  last hisr: 0004h, himr: 00002ABFh, inpace: 0000h
  utility: 6316h, txphthre: 1010h, rxtxdmathre: 2828h
  dmactrl: 0000E004h, earlyrxthre: 0000h, llcstop: 0000h
  reset: 0000h
  txhidescstart: 4B0A45C0h, txlodescstart: 00000000h
  rxdescstart: 4B0A4180h, srbctrl: 0038h, descipoll: 0100h
  congestcnt: 0000h
Hawkeye transmit error counts:
  Underrun: 0/0
Hawkeye receive error counts:
  Out of descriptors: 0/0, Giants: 0/0
  Corrupted frames: 0/0, CRC errors: 0/0
  FIFO overflow: 0/0
Device driver ring buffer data:
  Transmit ring:
    Descriptors outstanding (curr/max): 0/256
    Head pointer: 7   Tail pointer: 7
  Receive ring:
    Ring size: 64 descriptors
    Head pointer: 7
Internal controller soft error counts:
  Line errors: 0/0, Internal errors: 0/0
  Burst errors: 0/0, ARI/FCI errors: 0/0
  Abort errors: 0/0, Lost frame errors: 0/0
  Copy errors: 0/0, Receiver congestion: 0/0
  Token errors: 0/0, Frequency errors: 0/0
Internal controller SMT state:
  Adapter MAC:     0008.2a36.1a04, Physical drop:       00000000
  NAUN address:    0060.3ebb.0a21, NAUN drop:           00000000
  Last beacon src: 0000.0000.0000, Last poll:           0060.3ebb.0a21
  Last MVID:       0006,           Last attn code:      0000
  Txmit priority:  0007,           Auth funct class:    FFFF
  Monitor error:   0000,           Front end errors:    0000
  Correlator:      0000,           Soft error timer:    00C8
  Local ring:      0000,           Ring status:         0000
  Beacon rcv type: 0000,           Beacon txmit type:   0000
  Last beacon type:0000,           Bcn station NAUN:    0000.0000.0000
  Beacon drop:     00000000,       Phantom support:     0000
  Access prot req: 0000,           Access prot resp:    0000
  Policy flags:    0110,           Protocol event state:000D
  Ctrl ring state: 0001,           Protocol join state: 0000
  Reserved:        0000,           Protocol mon state:  0000
```

The table below describes the significant fields shown in the display.

Table 89: show controllers token Field Descriptions

Field	Description
Tokenring4/0	Interface processor type, slot, and port.

Field	Description
Last Ring Status	Last abnormal ring condition. Can be any of the following: • Signal Loss • HW Removal • Remote Removal • Counter Overflow • Only station • Ring Recovery
Current operating mode	Operating mode. Can be one of the following: • Classic token ring station (standard half-duplex Token Ring station) • DTR station (full-duplex Token Ring station) • DTR concentrator (concentrator port)
MAC state	The MAC state indicates the state of the Token Ring MAC layer protocol. Can be one of the following: • Not inserted (not connected to any ring) • Inserting (currently entering a ring) • Inserted (connected to an active Token ring)

Related Commands

Command	Description
show interfaces tokenring	Displays information about the Token Ring interface and the state of source-route bridging.
show source-bridge	Displays the current source bridge configuration and miscellaneous statistics.

show controllers vg-anylan

To display the controller information for the 100VG-AnyLAN port adapter on Cisco 7200 series routers and Cisco 7500 series routers, use the **showcontrollersvg-anylan** command in user EXEC or privileged EXEC mode.

Cisco 7200 Series
show controllers vg-anylan *slot/port*

Cisco 7500 Series with VIP Cards
show controllers vg-anylan *slot/port-adapter/port*

Syntax Description

slot	Slot number. Refer to the appropriate hardware manual for slot and port information.
/ *port*	Port number. Refer to the appropriate hardware manual for slot and port information.
/ *port-adapter*	Port adapter number. Refer to the appropriate hardware manual for information about port adapter compatibility.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The information displayed is generally useful for diagnostic tasks performed by technical support personnel only.

Examples

The following is sample output from the **showcontrollersvg-anylan** command:

```
Router# show controllers vg-anylan 3/0
Interface VG-AnyLAN3/0
Hardware is MC68852
 mc68852_ds=0x60A4C930, registers=0x3C300000, ib=0x4B056240
 rx ring entries=31, tx ring entries=31
 rxring=0x4B056340, rxr shadow=0x60A4CA08, rx_head=0, rx_tail=0
 txring=0x4B057180, txr shadow=0x60A4D07C, tx_head=0, tx_tail=2,
tx_count=2,
MC68852 Registers:
 hw_id: 5048, hw_id & page: 7053, opr1=0x26, opr2=0x2C, opr3=0x00
  Page 0 - Performance:
  isr=0x3400, imr=0x0A0A, flreg=0x0000
  xfrct=0xC07E0080, rxcnt=0, txcnt=1F
  Page 1 - MAC Address/Hash Table:
  addrlow= 6009B9, addrhigh=9B1809B9,hash bytes=06 00 20 00 00 00 00 00
  Page 2 - Hardware Mapping:
  mmmsw=0x3785, mmlsw=0x0000, bmreg =0x04
```

```
 Page 4 - LAN Configuration:
 tccnf1=0x00, tccnf2=0x01
 vccnf=0x99, vtrrg=0x0020, valow1=0x0000, valow2=0x0000
 maccr1=0xBE, maccr2=0x00, maccr3=0x04, maccr4=0x03
 Page 5 - MMU Registers:
 rx mem stop addr=0xFF03, tx mem stop addr=0xFF07
MC68852 PCI registers:
 bus_no=6, device_no=0
 CFID=0x0005101A, CFCS=0x02800005, CFRV=0x02000000, CFLT=0x0000F800
 CBIO=0x00006001, CBMA=0x00000000, CFIT=0x20080100, CFDA=0x0000000C
Actel Hardware CAM Control Registers:
 CAM DEVICE BASE: 0x3C300800  Register Address: 0x3C300C00
 CSR: 0x8000  CAMCR: 0xFFFF
 USAR: 0000  MSAR: 0000  LSAR: 0000
 FIFOCR: 0x8000  WRMASK: 0x0080
 COMPARAND REG: 0000.0000.0000
 PERSISTENT SOURCE: 0x0   PERSISTENT DEST: 0xFD010000
ACTEL CAM PCI registers:
 bus_no=6, device_no=1
 CFID=0x555511AA, CFCS=0x04800003, CFRV=0xF0F0F001, CFLT=0x00000000
 CBIO=0x00006800, CBMA=0x00000000, CFIT=0x00000000, CFDA=0x00000000
 pak_to_host=0x0, filtered_pak=0
 throttled=0, enabled=0, disabled=0
 tx_carrier_loss=0
 fatal_tx_err=0, mult_ovfl=0
```

show controllers wanphy

T o display the SPA mode (LAN mode or WAN mode), alarms, and the J1 byte string value, use the **showcontrollerswanphy**commandin Privileged EXEC mode.

show controllers wanphy *slot*/*subslot*/*port*

Syntax Description

slot	The SIP slot number in which the Cisco 1-Port 10 Gigabit Ethernet LAN/WAN-PHY Shared Port Adapter has been installed.
subslot	The subslot number in which the Cisco 1-Port 10 Gigabit Ethernet LAN/WAN-PHY Shared Port Adapter has been installed.
port	The port number of the Cisco 1-Port 10 Gigabit Ethernet LAN/WAN-PHY Shared Port Adapter. **Note** There is only 1 port (0) in the Cisco 1-Port 10 Gigabit Ethernet LAN/WAN-PHY Shared Port Adapter.

Command Default

No default values are available.

Command Modes

Privileged EXEC Mode (EXEC)

Command History

Release	Modification
Cisco IOS XE Release 3.3.0S	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines

The **showcontrollerwanphy**command has been introduced on the Cisco ASR 1000 Series Router in Cisco IOS XE Release 3.3.0S. This command is used to display:

- LAN or WAN mode of operation in which the SPA is currently working
- Configured alarms and active alarms (if any)
- Remote J1 byte string value passed to check the connectivity from local SPA to the remote SPA
- SF-BER and SD-BER threshold values

Examples

The following example shows the output of **showcontrollerswanphy** command:

```
Router# show controllers wanphy 0/1/0
TenGigabitEthernet0/1/0
Mode of Operation: WAN Mode
SECTION
  LOF = 0             LOS    = 0                            BIP(B1) = 0
LINE
  AIS = 0             RDI    = 0          FEBE = 0          BIP(B2) = 0
PATH
  AIS = 0             RDI    = 0          FEBE = 0          BIP(B3) = 0
  LOP = 0             NEWPTR = 0          PSE  = 0          NSE     = 0
WIS ALARMS
  SER    = 0          FELCDP = 0          FEAISP = 0
```

```
  WLOS   = 0          PLCD   = 0
  LFEBIP = 0          PBEC   = 0
Active Alarms[All defects]: SWLOF LAIS PAIS SER
Active Alarms[Highest Alarms]: SWLOF
Alarm reporting enabled for: SF SWLOF B1-TCA B2-TCA PLOP WLOS
  Rx(K1/K2): 00/00  Tx(K1/K2): 00/00
  S1S0 = 00, C2 = 0x1A
PATH TRACE BUFFER: UNSTABLE
  Remote J1 Byte :
BER thresholds:  SD = 10e-6  SF = 10e-3
TCA thresholds:  B1 = 10e-6  B2 = 10e-6  B3 = 10e-6
```

Related Commands

Command	Description
clear controller wanphy	Clears the counter of alarms generated, and resets it back to zero.

show controllers wlan-controller

To show the Cisco Wireless Local Area Network (WLAN) controller network module on the router, use the **showcontrollerswlan-controller** command in privileged EXEC mode.

show controllers wlan-controller slot/unit

Syntax Description

slot/unit	Specifies the router slot and unit numbers for the WLAN controller network module.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(2)XA1	This command was introduced on the router software.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.

Examples

The following example shows how to display interface information for the WLAN controller network module:

```
Router# show controllers wlan-controllers 1/0
Interface wlan-controller1/0
Hardware is Intel 82559 FastEthernet
IDB: 67796B08, FASTSEND: 60E073CC, MCI_INDEX: 0

INSTANCE=0x67797BE8
  Rx Ring entries = 64
  Rx Shadow = 0x67797ED0
  Rx Ring = 0x2DCC1840
  Rx Ring Head = 5
  Rx Ring Last = 4
  Rx Buffer Descr = 0x2DCC3040
  Rx Buffer Descr Head = 5
  Rx Buffer Descr Last = 4
  Rx Shadow (malloc) = 0x67797ED0
  Rx Ring (malloc) = 0x2DCC1840
  Rx Buffer Descr (malloc) = 0x2DCC3040
  Tx Ring entries = 128
  Tx Shadow = 0x67798008
  Tx Shadow Head = 13
  Tx Shadow Tail = 13
  Tx Shadow Free = 128
  Tx Ring = 0x2DCFAA40
  Tx Head = 15
  Tx Last = 14
  Tx Tail = 15
  Tx Count = 0
  Tx Buffer Descr = 0x2DCF9080
  Tx Buffer Descr Head = 0
  Tx Buffer Descr Tail = 0
  Tx Shadow (malloc) = 0x67798008
  Tx Ring (malloc) = 0x2DCFAA40
```

```
  Tx Buffer Descr (malloc) = 0x2DCF9080

CONTROL AND STATUS REGISTERS (CSR)=0x4B000000
  SCB Intr Mask     = 00
  SCB CU/RU Cmd     = 00
  SCB Intr Status   = 00
  SCB CU Status     = 01
  SCB RU Status     = 04
  SCB General Ptr   = 00000000
  PORT              = 00000000
  EEPROM            = 0008
  FLASH             = 0002
  MDI               = 1821782D
  Rx Byte Count     = 00000608
  PMDR              = 80
  FC Cmd            = 00
  FC Threshold      = 03
  Early Rx          = 00
  General Status    = 07
  General Control   = 00

PHY REGISTERS
  Register 0x00:   1000  782D  02A8  0154  0501  45E1  0003  0000
  Register 0x08:   0000  0000  0000  0000  0000  0000  0000  0000
  Register 0x10:   0203  0000  0001  0000  0000  0000  0000  0000
  Register 0x18:   0001  0000  8B10  0000  0000  0000  0000  0000

HARDWARE STATISTICS
  Rx good frames:         69
  Rx CRC:                 0
  Rx alignment:           0
  Rx resource:            0
  Rx overrun:             0
  Rx collision detects:   0
  Rx short:               0
  Tx good frames:         13
  Tx maximum collisions:  0
  Tx late collisions:     0
  Tx underruns:           0
  Tx lost carrier sense:  0
  Tx deferred:            0
  Tx single collisions:   0
  Tx multiple collisions: 0
  Tx total collisions:    0
  FC Tx pause:            0
  FC Rx pause:            0
  FC Rx unsupported:      0

INTERRUPT STATISTICS
  CX  = 468239
  FR  = 2393445
  CNA = 0
  RNR = 0
  MDI = 0
  SWI = 0
  FCP = 0

Receive All Multicasts = enabled
Receive Promiscuous = disabled
Loopback Mode = disabled


Module Reset Statistics:
  CLI reset count = 0
```

```
CLI reload count = 0
Registration request timeout reset count = 0
Error recovery timeout reset count = 0
Module registration count = 1
```

show counters interface

To display the information about the interface counter, use the **showcountersinterface** command in user EXEC or privileged EXEC mode.

show counters interface *type mod/port* [**delta**]

Syntax Description

type	Interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **port-channel**, **pos**, **atm**, **null**, **tunnel**, and **ge-wan**
mod / port	Module and port number.
delta	(Optional) Displays the interface counters values since the last **clearcounters** command.

Command Default

This command has no default settings.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXE	This command was changed to support the **delta** keyword on the Supervisor Engine 720 only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **showcountersinterface** command is not supported on SVIs.

The **showcountersinterfacedelta**command displays a detailed list of the last-saved counter values.

Examples

This example shows how to display the information about the interface counter:

```
Router# show counters interface fastethernet 5/2
64 bit counters:
 0.                      rxHCTotalPkts = 1
 1.                      txHCTotalPkts = 1
 2.                    rxHCUnicastPkts = 0
 3.                    txHCUnicastPkts = 0
 4.                  rxHCMulticastPkts = 0
 5.                  txHCMulticastPkts = 0
 6.                  rxHCBroadcastPkts = 1
 7.                  txHCBroadcastPkts = 1
 8.                         rxHCOctets = 78
 9.                         txHCOctets = 78
10.                 rxTxHCPkts64Octets = 0
11.            rxTxHCPkts65to127Octets = 2
12.           rxTxHCPkts128to255Octets = 0
13.           rxTxHCPkts256to511Octets = 0
14.          rxTxHCpkts512to1023Octets = 0
```

```
15.         rxTxHCpkts1024to1518Octets = 0
16.                    txHCTrunkFrames = 0
17.                    rxHCTrunkFrames = 0
18.                     rxHCDropEvents = 0
32 bit counters:
 0.                   rxCRCAlignErrors = 0
 1.                   rxUndersizedPkts = 0
 2.                    rxOversizedPkts = 0
 3.                     rxFragmentPkts = 0
 4.                          rxJabbers = 0
 5.                       txCollisions = 0
 6.                         ifInErrors = 0
 7.                        ifOutErrors = 0
 8.                       ifInDiscards = 0
 9.                  ifInUnknownProtos = 0
10.                      ifOutDiscards = 0
11.            txDelayExceededDiscards = 0
12.                              txCRC = 0
13.                         linkChange = 1
14.                   wrongEncapFrames = 0
All Port Counters
 1.                          InPackets = 1
 2.                           InOctets = 78
 3.                        InUcastPkts = 0
 4.                        InMcastPkts = 0
 5.                        InBcastPkts = 1
 6.                         OutPackets = 1
 7.                          OutOctets = 78
 8.                       OutUcastPkts = 0
 9.                       OutMcastPkts = 0
10.                       OutBcastPkts = 1
11.                           AlignErr = 0
12.                             FCSErr = 0
13.                            XmitErr = 0
14.                             RcvErr = 0
15.                          UnderSize = 0
16.                          SingleCol = 0
17.                           MultiCol = 0
18.                            LateCol = 0
19.                       ExcessiveCol = 0
20.                       CarrierSense = 0
21.                              Runts = 0
22.                             Giants = 0
23.                         InDiscards = 0
24.                        OutDiscards = 0
25.                           InErrors = 0
26.                          OutErrors = 0
27.                      TrunkFramesTx = 0
28.                      TrunkFramesRx = 0
29.                         WrongEncap = 0
30.     Broadcast_suppression_discards = 0
31.     Multicast_suppression_discards = 0
32.       Unicast_suppression_discards = 0
33.                rxTxHCPkts64Octets = 0
34.            rxTxHCPkts65to127Octets = 2
35.           rxTxHCPkts128to255Octets = 0
36.           rxTxHCPkts256to511Octets = 0
37.          rxTxHCpkts512to1023Octets = 0
38.         rxTxHCpkts1024to1518Octets = 0
39.                         DropEvents = 0
40.                     CRCAlignErrors = 0
41.                     UndersizedPkts = 0
42.                      OversizedPkts = 0
43.                       FragmentPkts = 0
```

```
44.                           Jabbers = 0
45.                        Collisions = 0
46.             DelayExceededDiscards = 0
47.                       bpduOutlost = 0
48.                       qos0Outlost = 0
49.                       qos1Outlost = 0
50.                       qos2Outlost = 0
51.                       qos3Outlost = 0
52.                   bpduCbicOutlost = 0
53.                   qos0CbicOutlost = 0
54.                   qos1CbicOutlost = 0
55.                   qos2CbicOutlost = 0
56.                   qos3CbicOutlost = 0
57.                        bpduInlost = 0
58.                        qos0Inlost = 0
59.                        qos1Inlost = 0
60.                        qos2Inlost = 0
61.                        qos3Inlost = 0
62.                        qos4Inlost = 0
63.                        qos5Inlost = 0
64.                        qos6Inlost = 0
65.                        qos7Inlost = 0
66.                        pqueInlost = 0
67.                          Overruns = 0
68.                          maxIndex = 0
Router#
```

This example shows how to display the values for the interface counters since the last **clearcounters** command:

```
Router# show counters interface gigabitethernet 5/2 delta

Time since last clear
---------------------
1d08h
64 bit counters:
0. rxHCTotalPkts = 508473
1. txHCTotalPkts = 2366
2. rxHCUnicastPkts = 411611
3. txHCUnicastPkts = 193
4. rxHCMulticastPkts = 81868
5. txHCMulticastPkts = 2155
6. rxHCBroadcastPkts = 14994
7. txHCBroadcastPkts = 18
8. rxHCOctets = 36961992
.
.
.
Router#
```

Related Commands

Command	Description
clear counters	Clears the interface counters.

show diag

To display hardware and diagnostic information for a networking device, line card, processor, jacket card, chassis, or network module, use the **show diag** command in privileged EXEC mode.

show diag [*slot-number*] [{**details** | **summary**}]

Cisco 7304 Router
show diag [{*slot-number* | **chassis** | **subslot** *slot/subslot*}] [{**details** | **summary**}]

Shared Port Adapters
show diag [**subslot** *slot/subslot*] [{**details** | **summary**}]

Network Module
show diag [*slot-number*]

Cisco 10000 Series Router
show diag [*slot/subslot*] [{**details** | **summary**}] [**crashdump**]

Cisco uBR10012 Universal Broadband Router
show diag [{*slot/subslot* | *slot/subslot/port* | **summary**}]

Cisco uBR7225VXR and Cisco uBR7246VXR Universal Broadband Routers
show diag *slot*

Cisco ASR 1000 Series Aggregation Services Routers
show diag [{**all** | **chassis** | **slot** | **subslot**}] **eeprom**

Cisco 4400 Series Integrated Services Router
show diag [{**all** | **chassis** | **slot** | **subslot**}] **eeprom**

Syntax Description

slot-number	(Optional) Slot number of the interface. If a slot number is not specified, diagnostic information for all slots is displayed.
details	(Optional) Displays more details than the normal **show diag** output.
summary	(Optional) Displays a summary (one line per slot) of the chassis.
chassis	(Optional) Specifies the display of diagnostic information about the backplane, power supplies, and fan modules.

subslot *slot* / *subslot*	(Optional) **Shared Port Adapters** Specifies the display of diagnostic information about the shared port adapter (SPA), where: • *slot* --Chassis slot number. See the appropriate hardware manual for slot information. For SPA interface processor (SIP), refer to the platform-specific SPA hardware installation guide or the corresponding “Identifying Slots and Subslots for SIPs and SPAs” topic in the platform-specific SPA software configuration guide. • *subslot* --Secondary slot number on a SIP where a SPA is installed. See the platform-specific SPA hardware installation guide and the corresponding “Specifying the Interface Address on a SPA” topic in the platform-specific SPA software configuration guide for subslot information. (Optional) Specifies subslot location information for the connected network modules and interfaces.
slot / *subslot/port*	(Optional) **Cisco uBR10012 Universal Broadband Router** Displays diagnostic information about the specified line card, where: • *slot* --Slot number of the line card in the uBR10012 router. The range is 0 to 8. • *subslot* --Subslot of the half-height line card in the uBR10012 router. The value t is either 0 or 1. • *port* --Port number on the cable interface. Valid values are 0 to 4 (depending on the cable interface).
slot	(Optional) **Cisco uBR7225VXR and Cisco uBR7246VXR Universal Broadband Routers** Displays diagnostic information about the specified line card, where: • *slot* --Slot number of the line card in the Cisco uBR7225VXR or Cisco uBR7246VXR router. Cisco uBR7246VXR router: The range is 3 to 6. Cisco uBR7225VXR router: The range is 1 to 2.
all	(Optional) Displays all diagnostic information related to EEPROM.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.1CA	This command was introduced.
11.2	This command was integrated into Cisco IOS Release 11.2.

Release	Modification
11.2P	This command output was modified for the PA-12E/2FE port adapter, PA-E3 port adapter, and PA-T3 port adapter.
11.2GS	This command was implemented on the Cisco 12000 series Internet router.
11.3 XA	This command was integrated in Cisco IOS Release 11.3 XA.
12.0	This command was implemented on the Cisco AS5300.
12.0(5)XQ	This command was implemented on the Cisco 1750 router.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.
12.1(9)EX	This command was introduced on the Cisco 7300 series routers, and the *slot-number* argument and **chassis** keyword were added.
12.1(10)EX	This command was enhanced to display information about Field-Programmable Gate Array (FPGA) image versions on installed NSEs and line cards on Cisco 7304 routers.
12.2(11)YZ	Support was added for the 7300-CC-PA.
12.2(8)T	This command was implemented for AIC and WIC cards on the Cisco 2600 series routers and the Cisco 3600 series routers.
12.2(13)T	This command was implemented for the AIM-VPN/EPII and AIM-VPN/HPII cards on the Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745 routers.
12.2(15)ZJ	This command was implemented for the AIM-VPN/BPII card on the Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM routers.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S and implemented on the Cisco 7304 router.
12.3(4)T	Support for the AIM-VPN/BPII card on the Cisco 2600XM series was integrated into Cisco IOS Release 12.3(4)T.
12.2(20)S2	This command was integrated into Cisco IOS Release 12.2(20)S2 and the **subslot***slotsubslot*keyword and arguments were added to support SPAs on the Cisco 7304 router.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S and the **subslot***slotsubslot*keyword and arguments were added to support SIPs and SPAs on the Cisco 12000 series Internet router.
12.4(4)T	This command was implemented for the HWIC-1ADSL and HWIC-1ADSLI interface cards on the following platforms: Cisco 1800 (modular) series, Cisco 2800 series, and Cisco 3800 series routers.
12.4(9)T	This command was implemented for the NME-AON-K9= enhanced network module on the following platforms: Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3725, and Cisco 3745 routers.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was enhanced with a crashdump option to enable you to display crashdump files collected on the SIP. This was implemented on the Cisco 10000 series router for the PRE3 and PRE4.
12.2(33)SCC	The output for this command was modified to display the diagnostic mode for the Cisco uBR10-MC5X20H cable interface line card on the uBR10012 router, when the field diagnostic image is loaded.
12.2(33)SCD	This command was modified. Support was added for the Cisco uBR7225VXR and Cisco uBR7246VXR routers.
12.2(33)XNE	This command was modified. The **all** keyword was added.
12.2(33)SCG	This command was modified. The output was modified to display all hardware and EEPROM information, including PID and PCB information for the Cisco uBR10-MC5X20H cable interface line card on the Cisco uBR10012 router.
IOS XE 3.9S	This command was integrated into Cisco IOS XE Release 3.9S.

Usage Guidelines

Use this command to determine the type of hardware installed in your router and to show detailed hardware information and EEPROM version information.

This command displays information for the motherboard, WAN interface cards (WICs), voice interface cards (VICs), high-speed WICs (HWICs), ATM interface cards (AICs), advanced integration modules (AIMs), port adapters, shared port adapters (SPAs), modular services cards (MSCs), SPA interface processors (SIPs), and enhanced network modules (NME).

For the Cisco 7304 router, this command applies to NEs, line cards, MSCs, and SPAs.

- To display hardware information for an NSE, line card, or MSC in the specified slot, use the *slot-number*argument. For MSCs, using this argument displays information about the MSC and each of its installed SPAs.
- To display hardware information about the backplane, power supplies, and fan modules, use the **chassis** keyword.

Shared Port Adapter Usage Guidelines

- To display hardware information for an MSC or SIP only in a specified slot, use the *slot-number*argument.
- To display hardware information for a SPA only, use the **show diag subslot***slot*/*subslot*version of this command.

Cisco 10000 Series Router Usage Guidelines

The **crashdump** keyword of the **show diag** command enables you to display any crashdump files collected on the SIP. The SIP stores the crashdump files by a reference number from 1 to 60.

To view a crashdump file, do the following:

1. Determine the most recent crashdump number:
   a. Enter the show diag slot/subslot command.
   b. Look for the latest crashdump number in the following section of the command output:

```
Number of crashdumps : output number
```

   c. Enter the following command to view the crashdump file:

```
show diag slot/subslot crashdump number
```

Note The subslot value is always zero for the SIP.

Cisco uBR10012 Router Usage Guidelines

- In the command syntax, the argument *slot/subslot* refers to a half-height line-card on the Cisco uBR10012 Router.
- This command applies to all cable interface line cards. The output for this command additionally displays the diagnostic mode when the Cisco uBR10-MC5X20H line card is enabled with the Field Diagnostic image.

Examples

1-Port T3 Serial Port Adapter: Example

The following is a sample output from the **show diag** command for a 1-port T3 serial port adapter in chassis slot 1 on a Cisco 7200 series router:

```
Router# show diag 1

Slot 1:
        Physical slot 1, ~physical slot 0xE, logical slot 1, CBus 0
        Microcode Status 0x4
        Master Enable, LED, WCS Loaded
        Board is analyzed
        Pending I/O Status: None
        EEPROM format version 1
        VIP2 controller, HW rev 2.4, board revision D0
        Serial number: 04372053  Part number: 73-1684-03
        Test history: 0x00        RMA number: 00-00-00
        Flags: cisco 7000 board; 7500 compatible

        EEPROM contents (hex):
          0x20: 01 15 02 04 00 42 B6 55 49 06 94 03 00 00 00 00
          0x30: 68 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

        Slot database information:
        Flags: 0x4      Insertion time: 0x14A8 (5d02h ago)

        Controller Memory Size: 16 MBytes DRAM, 1024 KBytes SRAM

        PA Bay 0 Information:
                T3 Serial PA, 1 ports
```

```
EEPROM format version 1
HW rev FF.FF, Board revision UNKNOWN
Serial number: 4294967295  Part number: 255-65535-255
```

Cisco 12000 Series Internet Router: Example

The following is a sample output from the **show diag** command on a Cisco 12000 series Internet router:

```
Router# show diag 3

SLOT 3  (RP/LC 3 ): 4 Port Packet Over SONET OC-3c/STM-1 Multi Mode
  MAIN: type 33,  00-0000-00 rev 70 dev 0
        HW config: 0x01    SW key: 00-00-00
  PCA:  73-2147-02 rev 94 ver 2
        HW version 1.0  S/N 04499695
  MBUS: MBUS Agent (1)  73-2146-05 rev 73 dev 0
        HW version 1.1  S/N 04494882
        Test hist: 0x00    RMA#: 00-00-00    RMA hist: 0x00
  DIAG: Test count: 0x05000001    Test results: 0x00000000

  MBUS Agent Software version 01.27 (RAM) using CAN Bus A
  ROM Monitor version 00.0D
  Fabric Downloader version used 00.0D (ROM version is 00.0D)
  Board is analyzed
  Board State is Line Card Enabled (IOS  RUN )
  Insertion time: 00:00:10 (00:04:51 ago)
  DRAM size: 33554432 bytes
  FrFab SDRAM size: 67108864 bytes
  ToFab SDRAM size: 16777216 bytes
```

The following is a sample output from the **show diag** command with the **summary** keyword:

```
Router# show diag summary

SLOT 0  (RP/LC 0 ): Route Processor
SLOT 2  (RP/LC 2 ): 4 Port Packet Over SONET OC-3c/STM-1 Single Mode
SLOT 4  (RP/LC 4 ): 4 Port Packet Over SONET OC-3c/STM-1 Single Mode
SLOT 7  (RP/LC 7 ): 4 Port Packet Over SONET OC-3c/STM-1 Single Mode
SLOT 9  (RP/LC 9 ): 4 Port Packet Over SONET OC-3c/STM-1 Single Mode
SLOT 11 (RP/LC 11): 4 Port Packet Over SONET OC-3c/STM-1 Single Mode
SLOT 16 (CSC 0   ): Clock Scheduler Card
SLOT 17 (CSC 1   ): Clock Scheduler Card
SLOT 18 (SFC 0   ): Switch Fabric Card
SLOT 19 (SFC 1   ): Switch Fabric Card
SLOT 20 (SFC 2   ): Switch Fabric Card
SLOT 24 (PS A1   ): AC Power Supply
SLOT 26 (PS B1   ): AC Power Supply
SLOT 28 (TOP FAN ): Blower Module
SLOT 29 (BOT FAN ): Blower Module
```

The following is a sample output from the **show diag** command with the **details** keyword:

```
Router# show diag 4 details

SLOT 4  (RP/LC 4): 4 Port Packet Over SONET OC-3c/STM-1 Single Mode
  MAIN: type 33,  800-2389-01 rev 71 dev 16777215
        HW config: 0x00    SW key: FF-FF-FF
  PCA:  73-2275-03 rev 75 ver 3
        HW version 1.1  S/N 04529465
```

```
MBUS: MBUS Agent (1)  73-2146-06 rev 73 dev 0
      HW version 1.1  S/N 04541395
      Test hist: 0xFF    RMA#: FF-FF-FF    RMA hist: 0xFF
DIAG: Test count: 0x05000001    Test results: 0x00000000

EEPROM contents (hex):
00: 01 00 01 00  49 00 08 62  06 03 00 00  00 FF FF FF
10: 30 34 35 34  31 33 39 35  FF FF FF FF  FF FF FF FF
20: 01 01 00 00  00 00 00 FF  FF FF FF FF  FF FF FF FF
30: A5 FF A5 A5  A5 A5 FF A5  A5 A5 A5 A5  A5 A5 A5 A5
40: 00 21 01 01  00 49 00 08  E3 03 05 03  00 01 FF FF
50: 03 20 00 09  55 01 01 FF  FF FF 00 FF  FF FF FF FF
60: 30 34 35 32  39 34 36 35  FF FF FF FF  FF FF FF FF
70: FF FF FF FF  FF FF FF FF  05 00 00 01  00 00 00 00

MBUS Agent Software version 01.24 (RAM)
Fabric Downloader version 00.0D
Board is analyzed
Flags: 0x4
Board State is Line Card Enabled (IOS  RUN)
Insertion time: 00:00:10 (00:04:51 ago)
DRAM size: 33554432 bytes
FrFab SDRAM size: 67108864 bytes
ToFab SDRAM size: 16777216 bytes
```

ATM SAR AIM in a Cisco 3660: Example

The following is a sample output from the **show diag** command for one ATM Segmentation and Reassembly (SAR) AIM in a Cisco 3660 router:

```
Router# show diag 0

3660 Chassis type: ENTERPRISE

c3600 Backplane EEPROM:
 Hardware Revision        : 1.0
 Top Assy. Part Number    : 800-04740-02

.
.
.

ATM AIM: 1
 ATM AIM module with SAR only (no DSPs)
 Hardware Revision        : 1.0
 Top Assy. Part Number    : 800-03700-01
 Board Revision           : A0
 Deviation Number         : 0-0
 Fab Version              : 02
 PCB Serial Number        : JAB9801ABCD
```

NM-AIC-64 Installed in a Cisco 2611: Example

The following is a sample output from the **show diag** command for a Cisco 2611 router with the NM-AIC-64 installed.

```
Router# show diag
```

```
Slot 0:
C2611 2E Mainboard Port adapter, 2 ports
Port adapter is analyzed
Port adapter insertion time unknown
EEPROM contents at hardware discovery:
Hardware Revision : 2.3
PCB Serial Number : JAD044808SG (1090473337)
Part Number : 73-2840-13
RMA History : 00
RMA Number : 0-0-0-0
Board Revision : C0
Deviation Number : 0-0
EEPROM format version 4
EEPROM contents (hex):
0x00: 04 FF 40 00 92 41 02 03 C1 18 4A 41 44 30 34 34
0x10: 38 30 38 53 47 20 28 31 30 39 30 34 37 33 33 33
0x20: 37 29 82 49 0B 18 0D 04 00 81 00 00 00 00 42 43
0x30: 30 80 00 00 00 00 FF FF FF FF FF FF FF FF FF FF
0x40: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x50: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

Slot 1:
NM_AIC_64 Port adapter, 3 ports
Port adapter is analyzed
Port adapter insertion time unknown
EEPROM contents at hardware discovery:
Hardware Revision : 1.0
Part Number : 74-1923-01
Board Revision : 02
PCB Serial Number : DAN05060012
EEPROM format version 4
EEPROM contents (hex):
0x00: 04 FF 40 02 55 41 01 00 82 4A 07 83 01 42 30 32
0x10: C1 8B 44 41 4E 30 35 30 36 30 30 31 32 FF FF FF
0x20: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x30: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x40: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x50: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

The table below describes significant fields shown in the display.

Table 90: show diag (AIC) Field Descriptions

Field	Description
C2611 2E Mainboard Port adapter, 2 ports	Line card type; number of ports available.
Port adapter is analyzed	The system has identified the port adapter.
Port adapter insertion time	Elapsed time since insertion.
Hardware Revision	Version number of the port adapter.
PCB Serial Number	Serial number of the printed circuit board.
Part Number	Part number of the port adapter.

Field	Description
RMA History	Counter that indicates how many times the port adapter has been returned and repaired.
RMA Number	Return material authorization number, which is an administrative number assigned if the port adapter needs to be returned for repair.
Board Revision	Revision number (signifying a minor revision) of the port adapter.
Deviation Number	Revision number (signifying a minor deviation) of the port adapter.
EEPROM format version	Version number of the EEPROM format.
EEPROM contents (hex)	Dumps of EEPROM programmed data.

AIM-VPN in a Cisco 2611XM: Example

The following example shows how to obtain hardware information about an installed AIM-VPN on the Cisco 2611XM router.

Router# **show diag 0**

Encryption AIM 1:

Hardware Revision :1.0

Top Assy. Part Number :800-03700-01

Board Revision :A0

Deviation Number :0-0

Fab Version :02

PCB Serial Number :JAB9801ABCD

RMA Test History :00

RMA Number :0-0-0-0

RMA History :00

EEPROM format version 4

EEPROM contents (hex):

0x00:04 FF 40 03 0B 41 01 00 C0 46 03 20 00 0E 74 01

0x10:42 41 30 80 00 00 00 00 02 02 C1 8B 4A 41 42 39

0x20:38 30 31 41 42 43 44 03 00 81 00 00 00 00 04 00

0x30:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

0x40:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

0x50:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

0x60:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

0x70:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

The table below describes significant fields shown in the display.

Table 91: show diag (AIM-VPN) Field Descriptions

Field	Description
Hardware Revision	Version number of the port adapter.
Top Assy. Part Number	Part number of the port adapter.
Board Revision	Revision number (signifying a minor revision) of the port adapter.
Deviation Number	Revision number (signifying a minor deviation) of the port adapter.
PCB Serial Number	Serial number of the printed circuit board.
RMA Number	Return material authorization number, which is an administrative number assigned if the port adapter needs to be returned for repair.
RMA History	Counter that indicates how many times the port adapter has been returned and repaired.
EEPROM format version	Version number of the EEPROM format.
EEPROM contents (hex)	Dumps of EEPROM programmed data.

MSC-100 on the Cisco 7304 Router: Example

The following is a sample output from the **show diag** *slot-number* version of the command for an MSC-100 located in slot number 4 on a Cisco 7304 router. Information about the MSC is followed by information for its associated SPAs:

```
Router# show diag 4

Slot 4:
        7304-MSC-100 SPA Carrier Card Line Card
        Line Card state: Active
        Insertion time: 00:08:49 ago
        Bandwidth points: 4000000
        EEPROM contents at hardware discovery:
        Hardware Revision        : 0.18
        Boot Time out            : 0000
        PCB Serial Number        : CSJ07288905
        Part Number              : 73-8789-01
        Board Revision           : A0
        Fab Version              : 02
        RMA Test History         : 00
        RMA Number               : 0-0-0-0
        RMA History              : 00
        Deviation Number         : 0-0
        Product Number           : 7304-MSC-100
        Top Assy. Part Number    : 68-1163-04
        Manufacturing Test Data  : 00 00 00 00 00 00 00 00
        Field Diagnostics Data   : 00 00 00 00 00 00 00 00
        Calibration Data         : Minimum: 0 dBmV, Maximum: 0 dBmV
```

```
              Calibration values :
        EEPROM format version 4

        EEPROM contents (hex):
          0x00: 04 FF 40 04 50 41 00 12 46 00 00 C1 8B 43 53 4A
          0x10: 30 37 32 38 38 39 30 35 82 49 22 55 01 42 41 30
          0x20: 02 02 03 00 81 00 00 00 00 04 00 80 00 00 00 00
          0x30: CB 94 37 33 30 34 2D 4D 53 43 2D 31 30 30 20 20
          0x40: 20 20 20 20 20 20 87 44 04 8B 04 C4 08 00 00 00
          0x50: 00 00 00 00 00 C5 08 00 00 00 00 00 00 00 00 C8
          0x60: 09 00 00 00 00 00 00 00 00 00 C7 7C F6 44 3F 30
          0x70: 00 00 00 00 00 00 00 00 00 00 00 00 02 EE FF C8
          0x80: C8 37 26 05 DC 64 28 1E 37 26 09 C4 64 32 28 32
          0x90: DD 0C E4 64 32 28 43 24 2E E0 AA 82 64 F4 24 00
          0xA0: 00 00 00 00 00 00 F0 2E FF FF FF FF FF FF FF FF
          0xB0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0xC0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0xD0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0xE0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0xF0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x100: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x110: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x120: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x130: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x140: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x150: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x160: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x170: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x180: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x190: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x1A0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x1B0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x1C0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x1D0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x1E0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x1F0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

        FPGA information:
          Current FPGA version     : 00.23
          IOS bundled FPGA version : 00.23
        CPLD version     : 01.02

Subslot 4/1:
        Shared port adapter: SPA-4FE-7304, 4 ports
        State: ok
        Insertion time: 00:15:13 ago
        Bandwidth: 400000 kbps
        EEPROM contents:
```

NSE-100 on the Cisco 7304 Router: Example

The following example displays diagnostic information about the NSE-100 in slot 0 of a Cisco 7304 router:

```
Router# show diag 0

Slot 0/1:
        NSE Card state:Primary
        Insertion time:00:03:47 ago
C7300 NSE Mainboard EEPROM:
        Hardware Revision        :2.3
```

```
        PCB Serial Number        :CAB0532JYYT
        Part Number              :73-5198-02
        Board Revision           :A0
        Fab Version              :02
        RMA Test History         :00
        RMA Number               :0-0-0-0
        RMA History              :00
        Deviation Number         :0-0
        Product Number           :7300-NSE-100
        Top Assy. Part Number    :68-1002-02
        Manufacturing Test Data  :00 00 00 00 00 00 00 00
        Field Diagnostics Data   :00 00 00 00 00 00 00 00
        Calibration Data         :Minimum:0 dBmV, Maximum:0 dBmV
              Calibration values :
        EEPROM format version 4

        EEPROM contents (hex):
          0x00:04 FF 40 02 8B 41 02 03 C1 8B 43 41 42 30 35 33
          0x10:32 4A 59 59 54 82 49 14 4E 02 42 41 30 02 02 03
          0x20:00 81 00 00 00 00 04 00 80 00 00 00 00 CB 94 37
          0x30:33 30 30 2D 4E 53 45 2D 31 30 30 20 20 20 20 20
          0x40:20 20 20 87 44 03 EA 02 C4 08 00 00 00 00 00 00
          0x50:00 00 C5 08 00 00 00 00 00 00 00 00 C8 09 00 00
          0x60:00 00 00 00 00 00 00 C7 7C F6 44 3F 30 F6 44 3F
          0x70:30 F6 44 3F 30 00 00 00 00 07 08 64 32 28 37 26
          0x80:09 C4 5A 32 28 32 DD 0C E4 5A 2D 23 43 24 13 88
          0x90:64 32 28 65 BA 2E E0 AA 82 64 F4 24 00 00 00 00
          0xA0:00 00 00 EF 1C FF FF FF FF FF FF FF FF FF FF FF
          0xB0:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0xC0:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0xD0:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0xE0:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0xF0:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

C7300 NSE Daughterboard EEPROM:
        Hardware Revision        :2.0
        PCB Serial Number        :CAB0533K3PP
        Part Number              :73-5673-03
        Board Revision           :A0
        Fab Version              :03
        RMA Test History         :00
        RMA Number               :0-0-0-0
        RMA History              :00
        Deviation Number         :0-0
        Product Number           :7300-NSE-100
        Top Assy. Part Number    :68-1002-02
        Manufacturing Test Data  :00 00 00 00 00 00 00 00
        Field Diagnostics Data   :00 00 00 00 00 00 00 00
        Calibration Data         :Minimum:0 dBmV, Maximum:0 dBmV
              Calibration values :
        EEPROM format version 4
        EEPROM contents (hex):
          0x00:04 FF 40 02 8C 41 02 00 C1 8B 43 41 42 30 35 33
          0x10:33 4B 33 50 50 82 49 16 29 03 42 41 30 02 03 03
          0x20:00 81 00 00 00 00 04 00 80 00 00 00 00 CB 94 37
          0x30:33 30 30 2D 4E 53 45 2D 31 30 30 20 20 20 20 20
          0x40:20 20 20 87 44 03 EA 02 C4 08 00 00 00 00 00 00
          0x50:00 00 C5 08 00 00 00 00 00 00 00 00 C8 09 00 00
          0x60:00 00 00 00 00 00 00 C7 7C F6 44 3F 30 00 00 00
          0x70:00 00 00 00 00 00 00 00 00 06 72 64 1E 1C 37 26
          0x80:07 08 64 32 28 37 26 00 00 00 00 00 00 00 00 00
          0x90:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          0xA0:00 00 00 FB BA FF FF FF FF FF FF FF FF FF FF FF
          0xB0:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

```
          0xC0:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0xD0:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0xE0:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0xF0:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

        FPGA information:
          Current NSE MB FPGA version     :0.3
          IOS bundled NSE MB FPGA version :0.12
          Current NSE DB FPGA version     :0.3
          IOS bundled NSE DB FPGA version :0.10
Fault History Buffer:
7300 Software (C7300-IS-M), Experimental Version 12.1(20011206:191841) [user-ws1 179]
Compiled Tue 29-Jan-02 08:10 by
Signal = 22, Code = 0x0, Uptime 00:00:48
$0 :FFFFFFFF, AT :47001098, v0 :10020028, v1 :0000006F
a0 :A0000000, a1 :00000005, a2 :00000001, a3 :10020028
t0 :00000028, t1 :3401E101, t2 :34018100, t3 :FFFF00FF
t4 :40332E68, t5 :43204650, t6 :70646174, t7 :69707065
s0 :FFFFFFFF, s1 :FFFFFFFF, s2 :FFFFFFFF, s3 :FFFFFFFF
s4 :FFFFFFFF, s5 :FFFFFFFF, s6 :FFFFFFFF, s7 :FFFFFFFF
t8 :00000000, t9 :00000000, k0 :3041D001, k1 :30410000
gp :FFFFFFFF, sp :41AA8F20, s8 :FFFFFFFF, ra :4036B6A4
EPC :4036B69C, SREG :3401E103, Cause :FFFFFFFF
Error EPC :FFFFFFFF, BadVaddr :FFFFFFFF

ROMMON Last Error Info:
count:19,  reason:reset
pc:0x4020BFBC,  error address:0x00000000
Stack Trace:
FP:0x00000000, PC:0x00000000
FP:0x00000000, PC:0x00000000
```

Shared Port Adapters on the Cisco 7304 Router: Example

The following is a sample output from the **show diag subslot** command for a 4-Port 10/100 Fast Ethernet SPA located in the bottom subslot (1) of the MSC that is installed in slot 4 on a Cisco 7304 router:

```
Router# show diag subslot 4/1

Subslot 4/1:
        Shared port adapter: SPA-4FE-7304, 4 ports
        Info: hw-ver=0x100, sw-ver=0x0 fpga-ver=0x0
        State: ok
        Insertion time: 23:20:42 ago
        Bandwidth: 400000 kbps
        EEPROM contents:
        Hardware Revision        : 1.0
        Boot Time out            : 0190
        PCB Serial Number        : JAB073204G5
        Part Number              : 73-8717-03
        73/68 Level Revision     : 01
        Fab Version              : 02
        RMA Test History         : 00
        RMA Number               : 0-0-0-0
        RMA History              : 00
        Deviation Number         : 0
        Product Number           : SPA-4FE-7304
        Product Version Id       : V01
        Top Assy. Part Number    : 68-2181-01
        73/68 Level Revision     : A0
```

```
CLEI Code                 : CNS9420AAA
Base MAC Address          : 0000.0000.0000
MAC Address block size    : 1024
Manufacturing Test Data   : 00 00 00 00 00 00 00 00
Field Diagnostics Data    : 00 00 00 00 00 00 00 00
Field Diagnostics Data    : 00 00 00 00 00 00 00 00
                            00 00 00 00 00 00 00 00
                            00 00 00 00 00 00 00 00
                            00 00 00 00 00 00 00 00
                            00 00 00 00 00 00 00 00
                            00 00 00 00 00 00 00 00
                            00 00 00 00 00 00 00 00
                            00 00 00 00 00 00 00 00
                            00 00 00 00 00 00 00 00
                            00 00 00 00 00 00 00 00
                            00 00 00 00 00 00 00 00
                            00 00 00 00 00 00 00 00
                            00 00 00 00
Calibration Data          : Minimum: 0 dBmV, Maximum: 0 dBmV
      Calibration values :
Power Consumption         : 160000mW max
                  Mode 1 : 0mW
                  Mode 2 : 0mW
                  Mode 3 : 0mW
EEPROM format version 4
EEPROM contents (hex):
  0x00: 04 FF 40 04 35 41 01 00 46 01 90 C1 8B 4A 41 42
  0x10: 30 37 33 32 30 34 47 35 82 49 22 0D 03 8A 30 31
  0x20: 20 20 02 02 03 00 81 00 00 00 00 04 00 88 00 00
  0x30: 00 00 CB 94 53 50 41 2D 34 46 45 2D 37 33 30 34
  0x40: 20 20 20 20 20 20 20 20 89 56 30 31 20 87 44 08
  0x50: 85 01 8A 41 30 20 20 C6 8A 43 4E 53 39 34 32 30
  0x60: 41 41 41 CF 06 00 00 00 00 00 00 43 04 00 C4 08
  0x70: 00 00 00 00 00 00 00 00 C5 08 00 00 00 00 00 00
  0x80: 00 00 F4 00 64 00 00 00 00 00 00 00 00 00 00 00
  0x90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0xA0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0xB0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0xC0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0xD0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0xE0: 00 00 00 00 00 00 00 00 00 C8 09 00 00 00 00 00
  0xF0: 00 00 00 00 D7 08 3E 80 00 00 00 00 00 00 F3 00
  0x100: 41 01 08 F6 48 43 34 F6 49 44 35 02 31 04 B0 B4
  0x110: A0 8C 00 00 05 DC 64 46 32 00 00 07 08 64 46 32
  0x120: 00 00 09 C4 64 46 32 00 00 0C E4 64 46 32 00 00
  0x130: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FE 02
  0x140: F2 A6 FF FF FF FF FF FF FF FF FF FF FF FF FF FF
  0x150: CC A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x160: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x170: 00 00 D4 A0 00 00 00 00 00 00 00 00 00 00 00 00
  0x180: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x190: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x1A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x1B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x1C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x1D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x1E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x1F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
FPGA version:
  Software version : 04.17
  Hardware version : 04.17
```

The following is a sample output from the **show diag subslot** command for a 2-Port 10/100/1000 Gigabit Ethernet SPA located in the top subslot (0) of the MSC that is installed in slot 4 on a Cisco 7304 router:

```
Router# show diag subslot 4/0

Subslot 4/0:
Shared port adapter: SPA-2GE-7304, 2 ports
Info: hw-ver=0x17, sw-ver=0x0 fpga-ver=0x0
State: ok
Insertion time: 00:08:47 ago
Bandwidth: 2000000 kbps
EEPROM contents:
Hardware Revision : 0.23
Boot Time out : 0190
PCB Serial Number : JAB073406YH
Part Number : 73-8792-02
73/68 Level Revision : 01
Fab Version : 02
RMA Test History : 00
RMA Number : 0-0-0-0
RMA History : 00
Deviation Number : 0
Product Number : SPA-2GE-7304
Product Version Id : V01
Top Assy. Part Number : 68-2181-01
73/68 Level Revision : A0
CLEI Code : CNS9420AAA
Base MAC Address : 0000.0000.0000
MAC Address block size : 1024

Manufacturing Test Data : 00 00 00 00 00 00 00 00
Field Diagnostics Data :  00 00 00 00 00 00 00 00
Field Diagnostics Data :  00 00 00 00 00 00 00 00
                          00 00 00 00 00 00 00 00
                          00 00 00 00 00 00 00 00
                          00 00 00 00 00 00 00 00
                          00 00 00 00 00 00 00 00
                          00 00 00 00 00 00 00 00
                          00 00 00 00 00 00 00 00
                          00 00 00 00 00 00 00 00
                          00 00 00 00 00 00 00 00
                          00 00 00 00 00 00 00 00
                          00 00 00 00 00 00 00 00
                          00 00 00 00 00 00 00 00
                          00 00 00 00

Calibration Data : Minimum: 0 dBmV, Maximum: 0 dBmV
Calibration values :
Power Consumption : 160000mW max
Mode 1 : 0mW
Mode 2 : 0mW
Mode 3 : 0mW

EEPROM format version 4
EEPROM contents (hex):
0x00: 04 FF 40 04 36 41 00 17 46 01 90 C1 8B 4A 41 42
0x10: 30 37 33 34 30 36 59 48 82 49 22 58 02 8A 30 31
0x20: 20 20 02 02 03 00 81 00 00 00 00 04 00 88 00 00
0x30: 00 00 CB 94 53 50 41 2D 32 47 45 2D 37 33 30 34
0x40: 20 20 20 20 20 20 20 20 89 56 30 31 20 87 44 08
0x50: 85 01 8A 41 30 20 20 C6 8A 43 4E 53 39 34 32 30
0x60: 41 41 41 CF 06 00 00 00 00 00 00 43 04 00 C4 08
```

```
0x70: 00 00 00 00 00 00 00 00 C5 08 00 00 00 00 00 00
0x80: 00 00 F4 00 64 00 00 00 00 00 00 00 00 00 00 00
0x90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xA0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xB0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xC0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xD0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xE0: 00 00 00 00 00 00 00 00 00 C8 09 00 00 00 00 00
0xF0: 00 00 00 00 D7 08 3E 80 00 00 00 00 00 00 F3 00
0x100: 41 01 08 F6 48 43 34 F6 49 44 35 02 31 03 E8 B4
0x110: A0 8C 37 26 05 DC 64 46 32 37 26 07 08 64 46 32
0x120: 37 26 09 C4 64 46 32 32 DD 0C E4 64 46 32 43 24
0x130: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FE 02
0x140: EF E2 FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x150: CC A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x160: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x170: 00 00 D4 A0 00 00 00 00 00 00 00 00 00 00 00 00
0x180: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x190: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x1A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x1B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x1C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x1D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x1E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x1F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

FPGA version:
Software version : 04.17
Hardware version : 04.17
```

Shared Port Adapter on a Cisco 12000 Series Internet Router: Example

The following is a sample output from the **show diag subslot** command for the 1-Port OC-192c/STM-64c POS/RPR XFP SPA in subslot 1 of the SIP located in chassis slot 1 on a Cisco 12000 series Internet router:

```
Router# show diag subslot 1/1

SUBSLOT  1/1 (SPA-OC192POS-XFP): 1-port OC192/STM64 POS/RPR XFP Optics Shared Port Adapter
       Product Identifier (PID) : SPA-OC192POS-XFP
       Version Identifier (VID) : V01
       PCB Serial Number        : PRTA1304061
       Top Assy. Part Number    : 68-2190-01
       Top Assy. Revision       : A0
       Hardware Revision        : 2.0
       CLEI Code                : UNASSIGNED
       Insertion Time           : 00:00:10 (13:14:17 ago)
       Operational Status       : ok
```

The table below describes the significant fields shown in the display.

Table 92: show diag subslot Field Descriptions for Cisco 12000 Series Internet Routers

Field	Description
Product Identifier (PID)	Product number of the SPA.
Version Identifier (VID)	Version number of the SPA.
PCB Serial Number	Serial number of the printed circuit board.

Field	Description
Top Assy. Part Number	Part number of the SPA.
Top Assy. Revision	Revision number (signifying a minor revision) of the SPA.
Hardware Revision	Revision number (signifying a minor revision) of the SPA hardware.
CLEI Code	Common Language Equipment Identification number.
Insertion Time	Time when the SPA was installed, and elapsed time between that insertion time and the current time.
Operational Status	Current status of the SPA. For more information about the status field descriptions, refer to the **show hw-module subslot oir** command.

The following is a sample output from the **show diag subslot details**command for the 1-Port OC-192c/STM-64c POS/RPR XFP SPA in subslot 1 of the SIP located in chassis slot 1 on a Cisco 12000 series Internet router:

```
Router# show diag subslot 1/1 details

SUBSLOT  1/1 (SPA-OC192POS-XFP): 1-port OC192/STM64 POS/RPR XFP Optics Shared Port Adapter
       EEPROM version           : 4
       Compatible Type          : 0xFF
       Controller Type          : 1100
       Hardware Revision        : 2.0
       Boot Timeout             : 400 msecs
       PCB Serial Number        : PRTA1304061
       PCB Part Number          : 73-8546-01
       PCB Revision             : A0        Fab Version              : 01
       RMA Test History         : 00
       RMA Number               : 0-0-0-0
       RMA History              : 00
       Deviation Number         : 0
       Product Identifier (PID) : SPA-OC192POS-XFP
       Version Identifier (VID) : V01
       Top Assy. Part Number    : 68-2190-01
       Top Assy. Revision       : A0        IDPROM Format Revision   : 36
       System Clock Frequency   : 00 00 00 00 00 00 00 00
                                  00 00 00 00 00 00 00 00
                                  00 00 00 00 00 00
       CLEI Code                : UNASSIGNED
       Base MAC Address         : 00 00 00 00 00 00
       MAC Address block size   : 0
       Manufacturing Test Data  : 00 00 00 00 00 00 00 00
       Field Diagnostics Data   : 00 00 00 00 00 00 00 00
       Calibration Data         : Minimum: 0 dBmV, Maximum: 0 dBmV
             Calibration values :
       Power Consumption        : 11000 mWatts (Maximum)
       Environment Monitor Data : 03 30 04 B0 46 32 07 08
                                  46 32 09 C4 46 32 0C E4
                                  46 32 13 88 46 32 07 08
                                  46 32 EB B0 50 3C 00 00
                                  00 00 00 00 00 00 00 00
                                  00 00 00 00 00 00 00 00
                                  00 00 FE 02 F6 AC
       Processor Label          : 00 00 00 00 00 00 00
       Platform features        : 00 00 00 00 00 00 00 00
                                  00 00 00 00 00 00 00 00
```

```
                                 00 00 00 00 00 00 00 00
                                 00 00 00 00 00 00 00
        Asset ID               :
        Asset Alias            :
        Insertion Time         : 00:00:10 (13:14:24 ago)
        Operational Status     : ok
```

SPA Interface Processor on a Cisco 12000 Series Internet Router: Example

The following is a sample output from the **show diag** command for a SIP located in chassis slot 2 on a Cisco 12000 series Internet router:

```
Router# show diag 2

SLOT 2  (RP/LC 2 ): Modular 10G SPA Interface Card
  MAIN: type 149,  800-26270-01 rev 84
        Deviation: 0
        HW config: 0x00    SW key: 00-00-00
  PCA:  73-9607-01 rev 91 ver 1
        Design Release 1.0  S/N SAD08460678
  MBUS: Embedded Agent
        Test hist: 0x00    RMA#: 00-00-00    RMA hist: 0x00
  DIAG: Test count: 0x00000000    Test results: 0x00000000
  FRU:  Linecard/Module: 12000-SIP-650
  FRU:  Linecard/Module: 12000-SIP-650
        Processor Memory: MEM-LC5-1024=(Non-Replaceable)
        Packet Memory: MEM-LC5-PKT-256=(Non-Replaceable)
  L3 Engine: 5 - ISE OC192 (10 Gbps)
  MBUS Agent Software version 1.114 (RAM) (ROM version is 3.4)
  ROM Monitor version 255.255
  Fabric Downloader version used 3.7 (ROM version is 255.255)
  Primary clock is CSC 1
  Board is analyzed
  Board State is Line Card Enabled (IOS  RUN )
  Insertion time: 1d00h (2d08h ago)
  Processor Memory size: 1073741824 bytes
  TX Packet Memory size: 268435456 bytes, Packet Memory pagesize: 32768 bytes
  RX Packet Memory size: 268435456 bytes, Packet Memory pagesize: 32768 bytes
  0 crashes since restart
  SPA Information:
        subslot 2/0: SPA-OC192POS-XFP (0x44C), status is ok
        subslot 2/1: Empty
        subslot 2/2: Empty
        subslot 2/3: Empty
```

ADSL HWICs: Example

The following is a sample output from the **show diag** command for a Cisco 2811 router with HWIC-1ADSL installed in slot 1 and HWIC-1ADSLI installed in slot 2. Each HWIC has a daughtercard as part of its assembly. The command results below give the output from the HWIC followed by the output from its daughtercard.

Router# **show diag 0**

Slot 0:

```
C2811 Motherboard with 2FE and integrated VPN Port adapter, 2 ports
        Port adapter is analyzed
```

```
        Port adapter insertion time unknown
        Onboard VPN             : v2.2.0
        EEPROM contents at hardware discovery:
        PCB Serial Number        : FOC09052HHA
        Hardware Revision        : 2.0
        Top Assy. Part Number    : 800-21849-02
        Board Revision           : B0
        Deviation Number         : 0
        Fab Version              : 06
        RMA Test History         : 00
        RMA Number               : 0-0-0-0
        RMA History              : 00
        Processor type           : 87
        Hardware date code       : 20050205
        Chassis Serial Number    : FTX0908A0B0
        Chassis MAC Address      : 0013.1ac2.2848
        MAC Address block size   : 24
        CLEI Code                : CNMJ7N0BRA
        Product (FRU) Number     : CISCO2811
        Part Number              : 73-7214-09
        Version Identifier       :   NA
        EEPROM format version 4
        EEPROM contents (hex):
          0x00: 04 FF C1 8B 46 4F 43 30 39 30 35 32 48 48 41 40
          0x10: 03 E7 41 02 00 C0 46 03 20 00 55 59 02 42 42 30
          0x20: 88 00 00 00 00 02 06 03 00 81 00 00 00 00 04 00
          0x30: 09 87 83 01 31 F1 1D C2 8B 46 54 58 30 39 30 38
          0x40: 41 30 42 30 C3 06 00 13 1A C2 28 48 43 00 18 C6
          0x50: 8A 43 4E 4D 4A 37 4E 30 42 52 41 CB 8F 43 49 53
          0x60: 43 4F 32 38 31 31 20 20 20 20 20 20 82 49 1C 2E
          0x70: 09 89 20 20 4E 41 D9 02 40 C1 FF FF FF FF FF FF

WIC Slot 1:
        ADSL over POTS
        Hardware Revision        : 7.0
        Top Assy. Part Number    : 800-26247-01
        Board Revision           : 01
        Deviation Number         : 0
        Fab Version              : 07
        PCB Serial Number        : FHH093600D4
        RMA Test History         : 00
        RMA Number               : 0-0-0-0
        RMA History              : 00
        Product (FRU) Number     : HWIC-1ADSL
        Version Identifier       : V01
        CLEI Code                :
        EEPROM format version 4
        EEPROM contents (hex):
          0x00: 04 FF 40 04 C8 41 07 00 C0 46 03 20 00 66 87 01
          0x10: 42 30 31 88 00 00 00 00 02 07 C1 8B 46 48 48 30
          0x20: 39 33 36 30 30 44 34 03 00 81 00 00 00 00 04 00
          0x30: CB 94 48 57 49 43 2D 31 41 44 53 4C 20 20 20 20
          0x40: 20 20 20 20 20 20 89 56 30 31 20 D9 02 40 C1 C6
          0x50: 8A FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
        EM Slot 0:
        ADSL over POTS non-removable daughtercard
        Hardware Revision        : 5.0
        Part Number              : 73-9307-05
        Board Revision           : 03
        Deviation Number         : 0
        Fab Version              : 05
        PCB Serial Number        : FHH0936006E
```

```
        RMA Test History         : 00
        RMA Number               : 0-0-0-0
        RMA History              : 00
        Fab Part Number          : 28-6607-05
        Manufacturing Test Data  : 00 00 00 00 00 00 00 00
        Field Diagnostics Data   : 00 00 00 00 00 00 00 00
        Connector Type           : 01
        Version Identifier       : V01
        Product (FRU) Number     :
        EEPROM format version 4
        EEPROM contents (hex):
          0x00: 04 FF 40 04 7A 41 05 00 82 49 24 5B 05 42 30 33
          0x10: 88 00 00 00 00 02 05 C1 8B 46 48 48 30 39 33 36
          0x20: 30 30 36 45 03 00 81 00 00 00 00 04 00 85 1C 19
          0x30: CF 05 C4 08 00 00 00 00 00 00 00 00 C5 08 00 00
          0x40: 00 00 00 00 00 00 05 01 89 56 30 31 20 FF FF FF
          0x50: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

WIC Slot 2:
        ADSL over ISDN
        Hardware Revision        : 7.0
        Top Assy. Part Number    : 800-26248-01
        Board Revision           : 01
        Deviation Number         : 0
        Fab Version              : 07
        PCB Serial Number        : FHH093600DA
        RMA Test History         : 00
        RMA Number               : 0-0-0-0
        RMA History              : 00
        Product (FRU) Number     : HWIC-1ADSLI
        Version Identifier       : V01
        CLEI Code                :
        EEPROM format version 4
        EEPROM contents (hex):
          0x00: 04 FF 40 04 C9 41 07 00 C0 46 03 20 00 66 88 01
          0x10: 42 30 31 88 00 00 00 00 02 07 C1 8B 46 48 48 30
          0x20: 39 33 36 30 30 44 41 03 00 81 00 00 00 00 04 00
          0x30: CB 94 48 57 49 43 2D 31 41 44 53 4C 49 20 20 20
          0x40: 20 20 20 20 20 20 89 56 30 31 20 D9 02 40 C1 C6
          0x50: 8A FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
        EM Slot 0:
        ADSL over ISDN non-removable daughtercard
        Hardware Revision        : 5.0
        Part Number              : 73-9308-05
        Board Revision           : 03
        Deviation Number         : 0
        Fab Version              : 05
        PCB Serial Number        : FHH0936008M
        RMA Test History         : 00
        RMA Number               : 0-0-0-0
        RMA History              : 00
        Fab Part Number          : 28-6607-05
        Manufacturing Test Data  : 00 00 00 00 00 00 00 00
        Field Diagnostics Data   : 00 00 00 00 00 00 00 00
        Connector Type           : 01
        Version Identifier       : V01
        Product (FRU) Number     :
        EEPROM format version 4
        EEPROM contents (hex):
          0x00: 04 FF 40 04 7B 41 05 00 82 49 24 5C 05 42 30 33
```

```
0x10: 88 00 00 00 00 02 05 C1 8B 46 48 48 30 39 33 36
0x20: 30 30 38 4D 03 00 81 00 00 00 00 04 00 85 1C 19
0x30: CF 05 C4 08 00 00 00 00 00 00 00 00 C5 08 00 00
0x40: 00 00 00 00 00 00 05 01 89 56 30 31 20 FF FF FF
0x50: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

NME-AON-K9= Installed in a Cisco 3845: Example

The following is a sample output from the **show diag** command for an integrated-service-engine port adapter in slot 2 on a Cisco 3845 router:

```
Slot 2:
        Integrated Service Engine Port adapter, 1 port
        Port adapter is analyzed
        Port adapter insertion time unknown
        EEPROM contents at hardware discovery:
        Hardware Revision         : 1.0
        Top Assy. Part Number     : 800-28152-01
        Board Revision            : 03
        Deviation Number          : 0
        Fab Version               : 01
        PCB Serial Number         : FOC101430NK
        RMA Test History          : 00
        RMA Number                : 0-0-0-0
        RMA History               : 00
        Version Identifier        : NA
        CLEI Code                 : TDB
        Product (FRU) Number      : NME-AON-K9
        EEPROM format version 4
        EEPROM contents (hex):
          0x00: 04 FF 40 05 5B 41 01 00 C0 46 03 20 00 6D F8 01
          0x10: 42 30 33 88 00 00 00 00 02 01 C1 8B 46 4F 43 31
          0x20: 30 31 34 33 30 4E 4B 03 00 81 00 00 00 00 04 00
          0x30: 89 4E 41 00 00 D9 02 40 C1 C6 8A 54 44 42 00 00
          0x40: 00 00 00 00 00 CB 88 4E 4D 45 2D 52 56 50 4E FF
          0x50: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

The table below describes the significant fields shown in the display.

Table 93: show diag subslot Field Descriptions for Cisco 3845 Series Routers

Field	Description
Hardware Revision	Revision number (signifying a minor revision) of the SPA hardware.
Top Assy. Part Number	Part number of the SPA.
Product Identifier (PID)	Product number of the SPA.
Board Revision	Revision number of the circuit board in the module.
Deviation Number	Deviation number of the module.
Fab Version	Fabrication version of the module.

Field	Description
PCB Serial Number	Serial number of the printed circuit board.
Top Assy. Revision	Revision number (signifying a minor revision) of the SPA.
RMA Test History	History of RMA testing.
RMA Number	RMA number of the module.
RMA History	History of RMA on this module.
Version Identifier	Nonapplicable to this module.
CLEI Code	Common Language Equipment Identification number. (nonapplicable on this module)
Product (FRU) Number	Product identification number.
EEPROM Format Version	Version of EEPROM format.
EEPROM Contents	Contents of EEPROM output.

Cisco uBR10012 and uBR7200 Series Broadband Routers

The following is a sample output from the **show diag** command displaying diagnostic information for the cable clock card:

```
router# show diag

Clockcard:
 National clock card with T1 controller
 EEPROM contents at hardware discovery:
 Hardware Revision        :1.1
 Part Number              :800-05867-02
 Board Revision           :11
 Deviation Number         :0-0
 Fab Version              :02
 PCB Serial Number        :CAB04046NXV
 RMA Test History         :00
 RMA Number               :0-0-0-0
 RMA History              :00
 EEPROM format version 4
 EEPROM contents (hex):
   0x00:04 FF 40 01 AC 41 01 01 C0 46 03 20 00 16 EB 02
   0x10:42 31 31 80 00 00 00 00 02 02 C1 8B 43 41 42 30
   0x20:34 30 34 36 4E 58 56 03 00 81 00 00 00 00 04 00
```

The table below describes the fields displayed by the **show diag** command.

Table 94: show diag Field Descriptions for Cisco uBR10012 and uBR7200 Series Routers

Field	Description
National clock card with T1 controller	The system has identified the cable clock card.

Field	Description
EEPROM contents at hardware discovery	EEPROM programmed data present when the system identified the clock card.
Hardware Revision	Version number of the card.
Part Number	Part number of the card.
Board Revision	Revision number (signifying a minor revision) of the card.
Deviation Number	Revision number (signifying a minor deviation) of the card.
Fab Version	Manufacturing fabrication version number.
PCB Serial Number	Serial number of the printed circuit board.
RMA Test History	Counter indicating how many times diagnostics have been performed on this card.
RMA Number	Return material authorization number, which is an administrative number assigned if the card needs to be returned for repair.
RMA History	Counter indicating how many times the card has been returned and repaired.
EEPROM format version	Version number of the EEPROM format.
EEPROM contents (hex)	Dumps of EEPROM programmed data.

The following is a sample output from the **show diag** command displaying revision-level information for the cable line card (slot 6):

```
Router# show diag

Slot 6:
        MC11 port adapter, 1 port
        Port adapter is analyzed
        Port adapter insertion time 02:37:10 ago
        Hardware Revision        : 1.2
        Part Number              : 800-02455-02
        Board Revision           : 03
        Deviation Number         : 0-3
        Fab Version              : 03
        PCB Serial Number        : 00004500239
        RMA Test History         : 00
        RMA Number               : 0-0-0-0
        RMA History              : 00
        Calibration Data         : Minimum: -8 dBmV, Maximum: 8 dBmV
              Calibration values : 0x5D43 0x3F05 0x1794
        Unknown Field (type 0083): 83 FF FF FF
        EEPROM format version 4
        EEPROM contents (hex):
          0x00: 04 FF 40 00 F1 41 01 02 C0 46 03 20 00 09 97 02
          0x10: 42 30 33 80 00 00 00 03 02 03 C1 8B 30 30 30 30
          0x20: 34 35 30 30 32 33 39 03 00 81 00 00 00 00 04 00
          0x30: C8 09 F8 08 03 5D 43 3F 05 17 94 83 83 FF FF FF
          0x40: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

```
0x50: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

The table below describes the fields displayed by the **show diag** command for the cable line card (slot 6).

Table 95: show diag Field Descriptions for Cable Line Card

Field	Description
MC11 port adapter	Line card type.
Port adapter is analyzed	The system has identified the Cisco CMTS port adapter.
Port adapter insertion time	Elapsed time since insertion.
Hardware Revision	Version number of the Cisco CMTS port adapter.
Part Number	In the Cisco CMTS, the part number of the port adapter.
Board Revision	Revision number (signifying a minor revision) of the Cisco CMTS port adapter.
Deviation Number	Revision number (signifying a minor deviation) of the Cisco CMTS port adapter.
Fab Version	Manufacturing fabrication version number.
PCB Serial Number	Serial number of the printed circuit board.
RMA Test History	Counter indicating how many times diagnostics have been performed on this port adapter.
RMA Number	Return material authorization number, which is an administrative number assigned if port adapter needs to be returned for repair.
RMA History	Counter indicating how many times the port adapter has been returned and repaired.
Calibration Data	Input power calibration range.
Calibration values	Upstream port gain calibration constant.
Unknown Field (type)	Unrecognized EEPROM fields.
EEPROM format version	Version number of the EEPROM format.
EEPROM contents (hex)	Dumps of EEPROM programmed data.

Tip In Cisco IOS Release 12.1(12)EC, Release 12.2(8)BC1, and later releases, you can add a timestamp to **show** commands using the **exec prompt timestamp** command in line configuration mode.

The following is a sample output displaying information on the Cisco Ethernet SPA:

```
Router# show diag 1/0
```

```
SPA Information:
bay 1/0       SPA-5X1GE-V2         ok
SW Version 1.0
Expected Switchover Action: NO INFORMATION
Product Identifier (PID) : SPA-5X1GE-V2
Version Identifier (VID) : V02
PCB Serial Number        : JAE1224L5DQ
Top Assy. Part Number    : 68-2616-02
Top Assy. Revision       : B0
Hardware Revision        : 1.2
CLEI Code                : CNUIAWYAAA
No Transceiver  in slot 1 subslot 0 port 1 .
No Transceiver  in slot 1 subslot 0 port 2 .
No Transceiver  in slot 1 subslot 0 port 3 .
No Transceiver  in slot 1 subslot 0 port 4 .

ETHERNET SPA Information: // Output displaying the additional Ethernet SPA inforamtion//

slot/bay 1/0:

SPA-5X1GE-V2 card, 5 ports
Card is half slot size
Card is analyzed
Card detected 00:10:29 ago
Card uptime: Not Supported
Card idle time: Not Supported
Voltage status:
Nominal 3300mV, Current 3314mV
Nominal 2500mV, Current 2527mV
Nominal 1500mV, Current 1524mV
Nominal 1200mV, Current 1209mV

EERPOM contents, slot/bay 1/0:

Controller Type          : 1290
Hardware Revision        : 1.2
Boot Timeout             : 400 msecs
PCB Serial Number        : JAE1224L5DQ
PCB Part Number          : 73-10421-02
PCB Revision             : B0
Fab Version              : 01
RMA Test History         : 00
RMA Number               : 0-0-0-0
RMA History              : 00
Deviation Number         : 0

Product Identifier (PID) : SPA-5X1GE-V2
Version Identifier (VID) : V02
Top Assy. Part Number    : 68-2616-02
Top Assy. Revision       : B0
IDPROM Format Revision   : 36
System Clock Frequency   : 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00
CLEI Code                : CNUIAWYAAA
Base MAC Address         : 00 00 00 00 00 00
MAC Address block size   : 0
Manufacturing Test Data  : 00 00 00 00 00 00 00 00
Field Diagnostics Data   : 00 00 00 00 00 00 00 00
Calibration Data         : Minimum: 0 dBmV, Maximum: 0 dBmV

Calibration values :
Power Consumption        : 13100 mWatts (Maximum)
```

```
Environment Monitor Data : 03 30 0C E4 46 32 09 C4
46 32 05 DC 46 32 04 B0
46 32 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 FE 02 F9 9B
Processor Label          : 00 00 00 00 00 00 00
Platform features        : 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00
Asset ID                 :
Asset Alias              :

SPA Information:  //Output displaying the Ethernet SPA summary information.//

bay 1/1       SPA-1X10GE-L-V2      ok

SW Version 1.0
Expected Switchover Action: NO INFORMATION
Product Identifier (PID) : SPA-1X10GE-L-V2
Version Identifier (VID) : V02
PCB Serial Number        : JAE1209A3LA
Top Assy. Part Number    : 68-2614-02
Top Assy. Revision       : B0
Hardware Revision        : 1.2
CLEI Code                : IPUIA5VRAA
No Transceiver  in slot 1 subslot 1 port 0 .
ETHERNET SPA Information: //Output displaying the additional Ethernet SPA information//

slot/bay 1/1:

SPA-1XTENGE-XFP-V2 card, 1 ports
Card is half slot size
Card is analyzed
Card detected 00:10:33 ago
Card uptime: Not Supported
Card idle time: Not Supported

Voltage status:
Nominal 3300mV, Current 3307mV
Nominal 2500mV, Current 2524mV
Nominal 1500mV, Current 1518mV
Nominal 1200mV, Current 1212mV
Nominal 1800mV, Current 1807mV
Nominal 1200mV, Current 1223mV
Nominal 1800mV, Current 1797mV
Nominal 5000mV, Current 4990mV
Nominal -5200mV, Current -5233mV

EERPOM contents, slot/bay 1/1:

Controller Type          : 1292
Hardware Revision        : 1.2
Boot Timeout             : 400 msecs
PCB Serial Number        : JAE1209A3LA
PCB Part Number          : 73-10419-02
PCB Revision             : A0
Fab Version              : 02
RMA Test History         : 00
RMA Number               : 0-0-0-0
RMA History              : 00
Deviation Number         : 0
```

```
Product Identifier (PID) : SPA-1X10GE-L-V2
Version Identifier (VID) : V02
Top Assy. Part Number    : 68-2614-02
Top Assy. Revision       : B0
IDPROM Format Revision   : 36
System Clock Frequency   : 00 00 00 00 00 00 00 00
                           00 00 00 00 00 00 00 00
                           00 00 00 00 00 00

CLEI Code                : IPUIA5VRAA
Base MAC Address         : 00 00 00 00 00 00
MAC Address block size   : 0
Manufacturing Test Data  : 00 00 00 00 00 00 00 00
Field Diagnostics Data   : 00 00 00 00 00 00 00 00
Calibration Data         : Minimum: 0 dBmV, Maximum: 0 dBmV
Calibration values :
Power Consumption        : 17400 mWatts (Maximum)
Environment Monitor Data : 03 30 0C E4 46 32 09 C4
46 32 05 DC 46 32 04 B0
46 32 07 08 46 32 04 B0
46 32 07 08 46 32 13 88
46 32 EB B0 46 32 00 00
00 00 00 00 00 00 00 00
00 00 FE 02 F4 3B
Processor Label          : 00 00 00 00 00 00 00
Platform features        : 00 00 00 00 00 00 00 00
                           00 00 00 00 00 00 00 00
                           00 00 00 00 00 00 00 00
                           00 00 00 00 00 00 00
Asset ID                 :
Asset Alias              :
```

The following is a sample output displaying the Cisco Wideband SPA information:

```
Router# show diag 1/0

SPA Information:
bay 1/2 SPA-24XDS-SFP ok
SW Version 1.0
Expected Switchover Action: NO INFORMATION
Product Identifier (PID) : SPA-24XDS-SFP
Version Identifier (VID) : V01
PCB Serial Number : CAT11105RXX
Top Assy. Part Number : 68-2562-03
Top Assy. Revision : B0
Hardware Revision : 1.0
CLEI Code : IPUIA1JRAA
The Transceiver in slot 1 subslot 2 port 0 is ENABLED.
The Transceiver in slot 1 subslot 2 port 1 is ENABLED.

Wideband Information: //Output displaying the Wideband SPA information for slot/bay 1/2//

slot/bay 1/2:

24rfchannel-spa-1 card, 1 port + 1 redundant port
Card is half slot size
Card is analyzed
Card detected 00:07:51 ago
Card uptime: Not Supported
Card idle time: Not Supported
Voltage status: 3.3V (+3.286) NOMINAL 2.5V (+2.490) NOMINAL
1.2V (+1.196) NOMINAL  1.8V (+1.816) FIXED
```

```
EEPROM contents, slot/bay 1/2:

Controller Type          : 1198
Hardware Revision        : 1.0
Boot Timeout             : 500 msecs
PCB Serial Number        : CAT11105RXX
PCB Part Number          : 73-9597-03
PCB Revision             : A0
Fab Version              : 03
RMA Test History         : 00
RMA Number               : 0-0-0-0
RMA History              : 00
Deviation Number         : 90114

Product Identifier (PID) : SPA-24XDS-SFP
Version Identifier (VID) : V01
Top Assy. Part Number    : 68-2562-03
Top Assy. Revision       : B0
IDPROM Format Revision   : 36
System Clock Frequency   : 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00
CLEI Code                : IPUIA1JRAA
Base MAC Address         : 00 1A A1 32 79 72
MAC Address block size   : 1
Manufacturing Test Data  : 00 00 00 00 00 00 00 00
Field Diagnostics Data   : 00 00 00 00 00 00 00 00
Calibration Data         : Minimum: 0 dBmV, Maximum: 0 dBmV
Calibration values :

Power Consumption        : 14000 mWatts (Maximum)
Environment Monitor Data : 03 30 0C E4 46 32 09 C4
                           46 32 00 00 00 00 04 B0
                           46 32 00 00 00 00 07 08
                           46 32 00 00 00 00 00 00
                           00 00 00 00 00 00 00 00
                           00 00 00 00 00 00 00 00
                           00 00 FE 02 FA 6D

Processor Label          : 00 00 00 00 00 00 00
Platform features        : 00 00 00 00 00 00 00 00
                           00 00 00 00 00 00 00 00
                           00 00 00 00 00 00 00 00
                           00 00 00 00 00 00 00
Asset ID                 :
Asset Alias              :
```

The following is a sample output from the **show diag** command for a Cisco uBR10-MC5X20H cable line card on a Cisco uBR10012 router using Cisco IOS Release 12.2(33)SCG:

```
Router# show diag 6/0

Slot/Subslot 6/0:
5cable-mc520h-d card, 5 ports
Card is half slot size
Card is analyzed
Card detected 00:01:18 ago
Card uptime 0 days, 0 hours, 1 minutes, 42 seconds
Card idle time N/A
Voltage status: 5V Nominal 3.3V Nominal 2.5V Nominal EEPROM contents,

slot 6/0:
Controller Type : 1159
```

```
Hardware Revision : 5.0
Top Assy. Part Number : 800-25212-05
Board Revision : B0
Product Identifier (PID) : UBR10-MC5X20H-D
CLEI Code : IPUCAHEBAA
Deviation Number : 0
Fab Version : 05
PCB Serial Number : CAT10505HA9
RMA Test History : 00
RMA Number : 0-0-0-0
RMA History : 00
Version Identifier (VID) : V01

LCMON version, slot 6/0
IOS (tm) 7200 Software (UBR10KCLC-LC-M), Experimental Version
12.3(20060207:230254) [xxxxx-after_520h 103]
Compiled Thu 09-Feb-06 11:59 by xxxxx
Reset due to: power-on
Operational Image version, slot 6/0
Cisco IOS Software, 10000 Software (UBR10KCLC-LCK8-M), Version 12.2(32.9.8)SCG,
EXPERIMENTAL IMAGE ENGINEERING C10K_WEEKLY BUILD, synced to V122_32_8_SCG

Compiled Mon 02-Jul-12 17:20 by xxxxx
SW Version 1.0
Code MD5 D41D8CD98F00B204E9800998ECF8427E
FPGA MD5 00000000000000000000000000000000
Expected Switchover Action: NO INFORMATION
```

The table below describes the significant fields shown in the display.

Table 96: show diag Field Descriptions for Cable Line Card

Field	Description
Hardware Revision	Version number of the card.
Top Assy. Part Number	Part number of the port adapter.
Board Revision	Revision number (signifying a minor revision) of the Cisco CMTS port adapter.
CLEI Code	Common language equipment identifier codes that are used by Telcordia licenses to uniquely identify the telecommunication equipment in their network.
Deviation Number	Revision number (signifying a minor deviation) of the Cisco CMTS port adapter.
Fab Version	Manufacturing fabrication version number.
PCB Serial Number	Serial number of the printed circuit board.
RMA Test History	Counter indicating how many times diagnostics have been performed on this port adapter.
RMA Number	Return material authorization number, which is an administrative number assigned if port adapter needs to be returned for repair.

Field	Description
RMA History	Counter indicating how many times the port adapter has been returned and repaired.

Cisco uBR7225VXR and Cisco uBR7246VXR Universal Broadband Routers: Example

The following is a sample output from the **show diag** command for a Cisco uBR-MC88V cable interface line card, on a Cisco uBR7246VXR universal broadband router. The output shows that the diagnostic mode on the line card is enabled.

Router# show diag5

```
Slot 5:

        DOCSIS Modem Card (Universal) 8 Down/8 Up (F-connector) with
            Integrated Up-converter Port adapter, 2 ports
        Port adapter is analyzed
        Port adapter insertion time 3w1d ago
        EEPROM contents at hardware discovery:
        Controller Type          : 1653
        PCB Serial Number        : CSJ12514210
        Hardware Revision        : 6.5
        Top Assy. Part Number    : 800-17733-09
        Top Assy. Revision       : A0
        Product Identifier (PID) : UBR-MC88V
        Version Identifier (VID) : V04
        CLEI Code                : IPUIA5XRAA
        Deviation Number         : 0
        Fab Version              : 06
        RMA Test History         : 00
        RMA Number               : 0-0-0-0
        RMA History              : 00
        Licensing Transaction ID : 8
        EEPROM format version 4

        EEPROM contents (hex):
          0x00: 04 FF 40 06 75 C1 8B 43 53 4A 31 32 35 31 34 32
          0x10: 31 30 41 06 05 C0 46 03 20 00 45 45 09 8D 41 30
          0x20: 20 20 CB 89 55 42 52 2D 4D 43 38 38 55 89 56 30
          0x30: 34 20 C6 8A 49 50 55 49 41 35 58 52 41 41 88 00
          0x40: 00 00 00 02 06 03 00 81 00 00 00 00 04 00 8B 00
          0x50: 00 00 08 D9 03 40 C1 CB FF FF FF FF FF FF FF FF
          0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          0x90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          0xA0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          0xB0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          0xC0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          0xD0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          0xE0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
          0xF0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

        License                  : 8X8
        Calibration Data
```

```
Number of US points: 8
Number of freqs    : 3
                  measured gain
US  freq(kHz)    0db       1db       2db       4db       8db
 16db
 0   5000       34.8876   33.8322   32.7126   30.6040   26.4336
18.4096
 1   5000       34.8876   33.9016   32.7126   30.6342   26.6766
18.4096
 2   5000       35.3706   34.3750   33.3282   31.3718   27.2786
19.0466
 3   5000       35.3706   34.3750   33.3282   31.3626   27.1574
19.0466
 4   5000       35.7702   34.8876   33.8322   31.3902   27.3962
19.3112
 5   5000       35.3706   34.3750   33.3282   31.3532   26.9278
18.7344
 6   5000       35.8262   34.8876   33.8322   31.3992   27.5134
19.3112
 7   5000       34.8876   33.8322   32.7126   30.6242   26.5632
18.4096

                  measured gain
US  freq(kHz)    0db       1db       2db       4db       8db
 16db
 0  30000       32.1330   31.3626   30.5834   28.2632   24.0922
15.8262
 1  30000       32.7126   31.3992   30.6142   28.5760   24.4296
16.2078
 2  30000       33.3282   32.0502   31.3532   29.1476   24.9126
16.6738
 3  30000       33.3282   32.0502   31.3436   29.0630   24.8932
16.6240
 4  30000       33.3282   32.0502   31.3532   29.2424   25.0476
17.0212
 5  30000       32.7126   32.0502   30.6440   28.8658   24.5942
16.6240
 6  30000       33.3282   32.7126   31.3718   29.4198   25.2018
17.0212
 7  30000       32.7126   31.3810   30.6040   28.4732   24.2630
16.2078

                  measured gain
US  freq(kHz)    0db       1db       2db       4db       8db
 16db
 0  65000       29.8170   29.0630   28.0608   26.0302   21.8206
13.8322
 1  65000       30.6142   29.6032   28.5760   26.5632   22.2546
13.9016
 2  65000       31.3532   29.8276   29.1596   27.1574   22.8458
14.8876
 3  65000       31.3340   29.8062   28.9646   26.9278   22.6460
14.3750
 4  65000       31.3532   29.8170   29.1476   27.0630   22.8458
14.8876
 5  65000       30.6342   29.7842   28.7668   26.6926   22.4660
14.3750
 6  65000       31.3718   30.5938   29.4198   27.2936   23.0430
14.8876
 7  65000       30.6142   29.5240   28.5632   26.4336   22.2546
13.9016
```

The table below describes significant fields shown in the display.

Table 97: show diag Field Descriptions for Cisco uBR7225VXR and Cisco uBR7246VXR Series Routers

Field	Description
Controller Type	Line card type.
PCB Serial Number	Serial number of the printed circuit board.
Hardware Revision	Version number of the port adapter.
Top Assy. Part Number	Part number of the port adapter.
Top Assy. Revision	Revision number (signifying a minor revision) of the port adapter.
Product Identifier (PID)	Cisco product ID.
Version Identifier (VID)	Used to track the version of the customer orderable PID.
CLEI Code	Common language equipment identifier codes that are used by Telcordia licenses to uniquely identify the telecommunication equipment in their network.
Deviation Number	Revision number (signifying a minor deviation) of the port adapter.
Fab Version	Version number (signifying a major version) of the port adapter.
RMA Test History	Counter indicating the number of times the port adapter has been returned and repaired.
RMA Number	Return material authorization number. An administrative number assigned when the port adapter is returned for repair.
RMA History	Counter indicating the number of times the port adapter has been returned and repaired.
Licensing Transaction ID	License transaction identifier.
EEPROM contents (hex)	Dumps of EEPROM programmed data.
License	License type.
Calibration Data	Calibration data of upstream VGA chips.
Number of US points	Number of physical upstream channels supported by the port adapter.
Number of freqs	Number of upstream frequencies used in the upstream calibration process (5, 30, and 65 MHz).

Cisco ASR 1000 Series Aggregation Services Routers: Example

The following is a sample output from the **show diag** command for a Cisco ASR 1000 Series Router.

```
Router# show diag all eeprom

MIDPLANE EEPROM data:
```

```
        Product Identifier (PID) : ASR1006
        Version Identifier (VID) : V01
        PCB Serial Number        : NWG122200GZ
        Top Assy. Part Number    : 68-2584-05
        Hardware Revision        : 1.0
        Asset ID                 :
        CLEI Code                : COMUD00ARA

Power/Fan Module P0 EEPROM data:
        Product Identifier (PID) : ASR1006-PWR-AC
        Version Identifier (VID) : V01
        PCB Serial Number        : ART1226Q00L
        Hardware Revision        : 3.0
        Asset ID                 :
        CLEI Code                : COUPACBBAA

Power/Fan Module P1 EEPROM data:
        Product Identifier (PID) : ASR1006-PWR-AC
        Version Identifier (VID) : V01
        PCB Serial Number        : ART1226Q00Q
        Hardware Revision        : 3.0
        Asset ID                 :
        CLEI Code                : COUPACBBAA

Slot R0 EEPROM data:
        Product Identifier (PID) : ASR1000-RP1
        Version Identifier (VID) : V03
        PCB Serial Number        : JAE12056VBZ
        Top Assy. Part Number    : 68-2625-08
        Hardware Revision        : 1.0
        CLEI Code                : COUCAENCAC

Slot R1 EEPROM data:
        Product Identifier (PID) : ASR1000-RP1
        Version Identifier (VID) : V03
        PCB Serial Number        : JAE1225MQIY
        Top Assy. Part Number    : 68-2625-08
        Hardware Revision        : 1.0
        CLEI Code                : COUCAENCAC

Slot F0 EEPROM data:
        Product Identifier (PID) : ASR1000-ESP10
        Version Identifier (VID) : V03
        PCB Serial Number        : JAE1228OBVV
        Top Assy. Part Number    : 68-2633-10
        Hardware Revision        : 1.1
        CLEI Code                : COUCAERCAC

Slot F1 EEPROM data:
        Product Identifier (PID) : ASR1000-ESP10
        Version Identifier (VID) : V03
        PCB Serial Number        : JAE1227NNN1
        Top Assy. Part Number    : 68-2633-10
        Hardware Revision        : 1.1
        CLEI Code                : COUCAERCAC

Slot 0 EEPROM data:
        Product Identifier (PID) : ASR1000-SIP10
        Version Identifier (VID) : V03
        PCB Serial Number        : JAE1224L050
        Top Assy. Part Number    : 68-2629-07
        Hardware Revision        : 1.0
        CLEI Code                : COUCAEPCAC
```

```
Slot 1 EEPROM data is not initialized
Slot 2 EEPROM data is not initialized

SPA EEPROM data for subslot 0/0:
        Product Identifier (PID) : SPA-2X1GE-V2
        Version Identifier (VID) : V01
        PCB Serial Number        : JAE1227NK77
        Top Assy. Part Number    : 68-2707-02
        Top Assy. Revision       : B0
        Hardware Revision        : 1.0
        CLEI Code                : CNUIANBAAA

SPA EEPROM data for subslot 0/1:
        Product Identifier (PID) : SPA-2XOC3-POS
        Version Identifier (VID) : V01
        PCB Serial Number        : JAE1225M5AO
        Top Assy. Part Number    : 68-2168-01
        Top Assy. Revision       : J0
        Hardware Revision        : 1.0
        CLEI Code                : IPUIAFMRAA

SPA EEPROM data for subslot 0/2 is not available
SPA EEPROM data for subslot 0/3 is not available
SPA EEPROM data for subslot 1/0 is not available
SPA EEPROM data for subslot 1/1 is not available
SPA EEPROM data for subslot 1/2 is not available
SPA EEPROM data for subslot 1/3 is not available
SPA EEPROM data for subslot 2/0 is not available
SPA EEPROM data for subslot 2/1 is not available
SPA EEPROM data for subslot 2/2 is not available
SPA EEPROM data for subslot 2/3 is not available
```

The table below describes significant fields shown in the display.

Table 98: show diag Field Descriptions for Cisco ASR 1000 Series Routers

Field	Description
Asset ID	Power or fan module identifier.
CLEI Code	Common language equipment identifier codes that are used by licensees to uniquely identify the telecommunication equipment in their network.
Hardware Revision	Version number of the port adapter.
PCB Serial Number	Serial number of the printed circuit board.
Product Identifier (PID)	Cisco product ID.
Top Assy. Part Number	Part number of the port adapter.
Top Assy. Revision	Revision number (signifying a minor revision) of the port adapter.
Version Identifier (VID)	Used to track the version of the customer orderable PID.

Cisco 4400 Series Integrated Services Router: Example

The following is a sample output from**show diag all eeprom detail** for Cisco 4400 Series Integrated Services Router.

```
Router# show diag all eeprom detail

MIDPLANE EEPROM data:

        EEPROM version           : 4
        Compatible Type          : 0xFF
        PCB Serial Number        : FOC15520B7L
        Controller Type          : 1902
        Hardware Revision        : 1.0
        PCB Part Number          : 73-13854-02
        Top Assy. Part Number    : 800-36894-01
        Board Revision           : 05
        Deviation Number         : 123968
        Fab Version              : 02
        Product Identifier (PID) : ISR4451/K9
        Version Identifier (VID) : V01
        CLEI Code                : TDBTDBTDBT
        Processor type           : D0
        Chassis Serial Number    : FGL1601129D
        Chassis MAC Address      : 30f7.0d53.c7e0
        MAC Address block size   : 144
        Manufacturing Test Data  : 00 00 00 00 00 00 00 00
        Asset ID                 : P1B-R2C
Power/Fan Module P0 EEPROM data:

        EEPROM version           : 4
        Compatible Type          : 0xFF
        Controller Type          : 1509
        Unknown Field (type 00DF): 1.85.1.236.1
        Deviation Number         : 0
        PCB Serial Number        : DCA1547X037
        RMA Test History         : 00
        RMA Number               : 0-0-0-0
        RMA History              : 00
        Version Identifier (VID) : XXX
        Product Identifier (PID) : XXX-XXXX-XX
        CLEI Code                : 0000000000
        Environment Monitor Data : 41 01 C2 42 00 05 F8 00
                                   50 01 F4 1B 58 03 E8 1F
                                   4A 05 DC 21 34 07 D0 21
                                   FC 09 C4 22 60 0B B8 22
                                   92 0D AC 22 D8 0F A0 22
                                   F8 11 94 22 F6 13 88 23
                                   3C 15 7C 23 28 17 70 23
                                   00 19 64 22 D8 1B 58 22
                                   C4 1D 4C 22 BA 1F 40 22
                                   A6 21 34 22 9C 23 28 22
                                   92 25 1C 22 88 27 10 22
                                   60
        Board Revision           : P0
Power/Fan Module P1 EEPROM data is not initialized

Power/Fan Module P2 EEPROM data is not initialized

Slot R0 EEPROM data:

        EEPROM version           : 4
        Compatible Type          : 0xFF
```

```
        PCB Serial Number        : FOC15520B7L
        Controller Type          : 1902
        Hardware Revision        : 1.0
        PCB Part Number          : 73-13854-02
        Top Assy. Part Number    : 800-36894-01
        Board Revision           : 05
        Deviation Number         : 123968
        Fab Version              : 02
        Product Identifier (PID) : ISR4451/K9
        Version Identifier (VID) : V01
        CLEI Code                : TDBTDBTDBT
        Processor type           : D0
        Chassis Serial Number    : FGL1601129D
        Chassis MAC Address      : 30f7.0d53.c7e0
        MAC Address block size   : 144
        Manufacturing Test Data  : 00 00 00 00 00 00 00 00
        Asset ID                 : P1B-R2C
        Asset ID                 :
Slot F0 EEPROM data:

        EEPROM version           : 4
        Compatible Type          : 0xFF
        Controller Type          : 3567
        Hardware Revision        : 4.1
        PCB Part Number          : 73-12387-01
        MAC Address block size   : 15
        Chassis MAC Address      : aabb.ccdd.eeff
        Product Identifier (PID) : ISR4451-FP
        Version Identifier (VID) : V00
        PCB Serial Number        : FP123456789
        Asset ID                 :
Slot 0 EEPROM data:

        EEPROM version           : 4
        Compatible Type          : 0xFF
        Controller Type          : 1612
        Hardware Revision        : 4.1
        PCB Part Number          : 73-12387-01
        MAC Address block size   : 15
        Chassis MAC Address      : aabb.ccdd.eeff
        Product Identifier (PID) : ISR4451-NGSM
        Version Identifier (VID) : V00
        PCB Serial Number        : NGSM1234567
        Asset ID                 :
Slot 1 EEPROM data:

        EEPROM version           : 4
        Compatible Type          : 0xFF
        Controller Type          : 1612
        Hardware Revision        : 4.1
        PCB Part Number          : 73-12387-01
        MAC Address block size   : 15
        Chassis MAC Address      : aabb.ccdd.eeff
        Product Identifier (PID) : ISR4451-NGSM
        Version Identifier (VID) : V00
        PCB Serial Number        : NGSM1234567
        Asset ID                 :
Slot 2 EEPROM data:

        EEPROM version           : 4
        Compatible Type          : 0xFF
        Controller Type          : 1612
        Hardware Revision        : 4.1
        PCB Part Number          : 73-12387-01
```

```
        MAC Address block size   : 15
        Chassis MAC Address      : aabb.ccdd.eeff
        Product Identifier (PID) : ISR4451-NGSM
        Version Identifier (VID) : V00
        PCB Serial Number        : NGSM1234567
        Asset ID                 :
SPA EEPROM data for subslot 0/0:

        EEPROM version           : 5
        Compatible Type          : 0xFF
        Controller Type          : 1902
        Hardware Revision        : 2.2
        Boot Timeout             : 400 msecs
        PCB Serial Number        : JAB092709EL
        PCB Part Number          : 73-8700-01
        PCB Revision             : A0
        Fab Version              : 01
        RMA Test History         : 00
        RMA Number               : 0-0-0-0
        RMA History              : 00
        Deviation Number         : 78409
        Product Identifier (PID) : ISR4451-4X1GE
        Version Identifier (VID) : V01
        Top Assy. Part Number    : 68-2236-01
        Top Assy. Revision       : A0
        IDPROM Format Revision   : 36
        System Clock Frequency   : 00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00
        CLEI Code                : CNUIAHSAAA
        Base MAC Address         : 00 00 00 00 00 00
        MAC Address block size   : 0
        Manufacturing Test Data  : 00 00 00 00 00 00 00 00
        Field Diagnostics Data   : 00 00 00 00 00 00 00 00
        Calibration Data         : Minimum: 0 dBmV, Maximum: 0 dBmV
              Calibration values :
        Power Consumption        : 13100 mWatts (Maximum)
        Environment Monitor Data : 03 30 0C E4 46 32 09 C4
                                   46 32 05 DC 46 32 05 DC
                                   46 32 00 00 00 00 00 00
                                   00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00 00 00
                                   00 00 FE 02 F9 6E
        Processor Label          : 00 00 00 00 00 00 00
        Platform features        : 00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00 00
        Asset ID                 :
        Asset Alias              :
SPA EEPROM data for subslot 0/1 is not available

SPA EEPROM data for subslot 0/2 is not available

SPA EEPROM data for subslot 0/3 is not available

SPA EEPROM data for subslot 0/4 is not available

SPA EEPROM data for subslot 1/0 is not available

SPA EEPROM data for subslot 1/1 is not available

SPA EEPROM data for subslot 1/2 is not available
```

```
SPA EEPROM data for subslot 1/3 is not available
SPA EEPROM data for subslot 1/4 is not available
SPA EEPROM data for subslot 2/0 is not available
SPA EEPROM data for subslot 2/1 is not available
SPA EEPROM data for subslot 2/2 is not available
SPA EEPROM data for subslot 2/3 is not available
SPA EEPROM data for subslot 2/4 is not available
```

Related Commands

Command	Description
dsl operating-mode (ADSL)	Modifies the operating mode of the digital subscriber line for an ATM interface.
show c7300	Displays the types of hardware (processors, line cards, jacket cards, and so on) installed in the Cisco 7304 router slots, including the bundled Flash, and current FPGA versions.
show c7300 errorlog	Displays error information on a Cisco 7304 router.
show dsl interface atm	Shows all ADSL-specific information for a specified ATM interface.
showcontrollers fastethernet	Displays Fast Ethernet interface information, transmission statistics and errors, and applicable MAC destination address and VLAN filtering tables.
show controllers gigabitethernet	Displays Gigabit Ethernet interface information, transmission statistics and errors, and applicable MAC destination address and VLAN filtering tables.
show controllers integrated-service-engine	Displays controller information for integrated-service-engine network modules.
showinterfaces integrated-service-engine	Displays basic interface configuration information for integrated-service-engine network modules.

show diagnostic bootup level

To display the coverage level for the configured bootup diagnostics, use the **showdiagnosticbootuplevel**command in user EXEC or privileged EXEC mode.

show diagnostic bootup level

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	This command was introduced for the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command displays the bootup diagnostic level configured on the switch. The bootup diagnostic level determines which diagnostic tests will be performed when the device boots. The following bootup diagnostic levels can be displayed in the output of this command:

Level	Explanation
Bypass	The device performs no bootup diagnostic tests.
Complete	The device performs all diagnostic tests marked with attribute M (Minimal) or C (Complete) in the output of the **showdiagnosticcontentmodule** command.
Minimal	The device performs all diagnostic tests marked with attribute M (Minimal) in the output of the **showdiagnosticcontentmodule** command.

Examples

This example shows how to display the configured bootup diagnostic level:

```
Router# show diagnostic bootup level
Current Bootup Diagnostic Level = Complete
```

Related Commands

Command	Description
diagnostic bootup level	Sets the bootup diagnostic level.
show diagnostic content module	Displays the available diagnostic tests.

show diagnostic content module

To display information about available tests, including test ID, test attributes, and supported coverage test levels for each test and for all modules, use the **showdiagnosticcontentmodule**command in user EXEC or privileged EXEC mode.

show diagnostic content module {**all***listslot* | *slot/subslot*}

Syntax Description

all	Displays information about available tests for all modules.
list	List of modules in the following format: • Entries are separated by a comma, for example, 1,4,6-10. • Ranges are specified with a hyphen, for example, 1-4,6-10.
slot	Single module by slot number.
slot / *subslot*	Single submodule by slot number and subslot or bay within the module.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	This command was introduced for the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4. A health-monitoring (HM) test, TestAclFpgaMonitor, was introduced for ABA cards.

Usage Guidelines

For each available diagnostic test, a set of attributes is displayed as a series of characters in the Attributes field of the command output. An asterisk (*) in the character location indicates that the attribute is not applicable to the test. The following set of attributes is displayed:

Character	Attribute	Description
1	M	The test runs when the bootup diagnostic level is set to either Minimal or Complete.
	C	The test runs when the bootup diagnostic level is set to Complete.
2	B	The test runs when the **diagnosticstart***platform***testbasic** command is entered.
3	P	The test runs on a port, not the entire device (per-port test).
	V	The test runs on the entire device (per-device test).

Character	Attribute	Description
4	D	The test disrupts the network traffic (disruptive test).
	N	The test can be run when the system is online without disrupting the network traffic (nondisruptive test).
5	S	If the card under test is a standby card, only the standby card runs the test. The test does not run from the active card. If the card under test is an active card, the active card runs the test on itself.
6	X	The test is not an HM test.
7	F	The monitoring interval of the test cannot be modified by the user (fixed monitoring test).
8	E	The user cannot disable the test (always enabled test).
9	A	Monitoring is active for this test.
	I	Monitoring is inactive for this test.
10	R	The test cycles power to the line cards and reloads the supervisor engine.
11	K	The test resets the line card after completion.
12	T	The test shuts down all ports and reloads the supervisor engine.

If a test is configured to run periodically, the interval will be displayed in the Test Interval field of the command output in the format ddd hh:mm:ss.ms, indicating days, hours, minutes, seconds, and milliseconds. For example, the test interval of a test that will run every 15 minutes will be displayed as 000 00:15:00.00. The test interval of a test that will run every 14 days will be displayed as 014 00:00:00.00.

If a test failure is determined by multiple errors rather than a single error, the error threshold will be displayed in the Threshold field of the command output.

You can use the **showdiagnosticdescriptionmodule**command to see a detailed description of a diagnostic test.

Examples

The following example shows how to display the test suite, the monitoring interval, and test attributes for module 5:

```
Router# show diagnostic content module 5
Module 5: Supervisor Engine 2T 10GE w/ CTS (Active)
Diagnostics test suite attributes:
    M/C/* - Minimal bootup level test / Complete bootup level test / NA
      B/* - Basic ondemand test / NA
    P/V/* - Per port test / Per device test / NA
    D/N/* - Disruptive test / Non-disruptive test / NA
      S/* - Only applicable to standby unit / NA
      X/* - Not a health monitoring test / NA
      F/* - Fixed monitoring interval test / NA
      E/* - Always enabled monitoring test / NA
      A/I - Monitoring is active / Monitoring is inactive
      R/* - Power-down line cards and need reload supervisor / NA
      K/* - Require resetting the line card after the test has completed / NA
```

```
     T/* - Shut down all ports and need reload supervisor / NA
                                                     Test Interval   Thre-
ID   Test Name                            Attributes      day hh:mm:ss.ms shold
==== ================================== ============    =============== =====
1) TestScratchRegister -------------> ***N****A***    000 00:00:30.00 5
   2) TestSPRPInbandPing --------------> ***N****A***    000 00:00:15.00 10
   3) TestTransceiverIntegrity --------> **PD****I***    not configured  n/a
   4) TestActiveToStandbyLoopback -----> M*PDSX**I***    not configured  n/a
   5) TestLoopback --------------------> M*PD*X**I***    not configured  n/a
   6) TestTxPathMonitoring ------------> M**N****A***    000 00:00:02.00 10
   7) TestNewIndexLearn ---------------> M**N****I***    000 00:00:15.00 10
   8) TestDontConditionalLearn --------> M**N****I***    000 00:00:15.00 10
   9) TestBadBpduTrap -----------------> M**D*X**I***    not configured  n/a
  10) TestMatchCapture ----------------> M**D*X**I***    not configured  n/a
  11) TestProtocolMatchChannel --------> M**D*X**I***    not configured  n/a
  12) TestFibDevices ------------------> M**N****I***    000 00:00:15.00 10
  13) TestIPv4FibShortcut -------------> M**N****I***    000 00:00:15.00 10
  14) TestL3Capture2 ------------------> M**D*X**I***    not configured  n/a
  15) TestIPv6FibShortcut -------------> M**N****I***    000 00:00:15.00 10
  16) TestMPLSFibShortcut -------------> M**N****I***    000 00:00:15.00 10
  17) TestNATFibShortcut --------------> M**N****I***    000 00:00:15.00 10
  18) TestAclPermit -------------------> M**D*X**I***    not configured  n/a
  19) TestAclDeny ---------------------> M**D*X**I***    not configured  n/a
  20) TestQoSTcam ---------------------> M**D*X**I***    not configured  n/a
  21) TestL3VlanMet -------------------> M**D*X**I***    not configured  n/a
  22) TestIngressSpan -----------------> M**D*X**I***    not configured  n/a
  23) TestEgressSpan ------------------> M**D*X**I***    not configured  n/a
  24) TestNetflowInlineRewrite --------> C*PD*X**I***    not configured  n/a
  25) TestTrafficStress ---------------> ***D*X**I**T    not configured  n/a
  26) TestFibTcamSSRAM ----------------> ***D*X**IR**    not configured  n/a
  27) TestAsicMemory ------------------> ***D*X**IR**    not configured  n/a
  28) TestAclQosTcam ------------------> ***D*X**IR**    not configured  n/a
  29) TestNetflowTcam -----------------> ***D*X**IR**    not configured  n/a
  30) ScheduleSwitchover --------------> ***D*X**I***    not configured  n/a
  31) TestFirmwareDiagStatus ----------> M**N****I***    000 00:00:15.00 10
  32) TestAsicSync --------------------> ***N****A***    000 00:00:15.00 10
  33) TestUnusedPortLoopback ----------> **PN****A***    000 00:01:00.00 10
  34) TestErrorCounterMonitor ---------> ***N****A***    000 00:00:30.00 10
  35) TestPortTxMonitoring ------------> **PN****A***    000 00:01:15.00 5
  36) TestL3HealthMonitoring ----------> ***N**FEA***    000 00:00:05.00 10
  37) TestCFRW ------------------------> M*VN*X**I***    not configured  n/a
  38) TestRwEngineOverSubscription ----> ***N****I***    000 00:00:01.00 10
  39) TestAclFpgaMonitor --------------> ***N****A***    000 00:00:00.80 1
40) TestNVRAMBatteryMonitor ---------> ***N**F*A***    000 01:00:00.00 72
```

Note The HM test, TestAclFpgaMonitor, is applicable only for Aphrodite, Berytos, and Anteros (ABA) cards. This test is run to monitor the access control list (ACL) ternary content addressable memory (TCAM) reply status.

Note The HM test TestNVRAMBatteryMonitor monitors the NVRAM battery status and is applicable only to the Supervisor Engine 2T.

The table below describes the significant fields shown in the display.

Table 99: show diagnostic content module Field Descriptions

Field	Description
ID	Unique identifier of the diagnostic test.
Test Name	Name of the diagnostic test.
Attributes	Health state of the diagnostic.
Test Interval	Periodic interval at which the test is run.
Threshold	Maximum number of consecutive test failures required by the diagnostic test to take recovery action.

Related Commands

Command	Description
diagnostic bootup level	Sets the bootup diagnostic level.
diagnostic monitor	Configures the HM diagnostic testing.
diagnostic ondemand	Configures the on-demand diagnostics.
diagnostic schedule test	Sets the scheduling of test-based diagnostic testing for a specific module or schedules a supervisor engine switchover.
show diagnostic description module	Describes the diagnostic tests.

show diagnostic cns

To display the information about the CNS subject, use the **show diagnostic cns** command in user EXEC or privileged EXEC mode.

show diagnostic cns {**publish** | **subscribe**}

Syntax Description

publish	Displays the subject with which the diagnostic results is published.
subscribe	Displays the subscribed subjects.

Command Default

This command has no default settings.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

The CNS subsystem communicates with remote network applications through the CNS-event agent and follows the publish and subscribe model. An application sets itself up to receive events by subscribing to the approprate event subject name.

Examples

This example shows how to display the subject with which the diagnostic results is published:

```
Router# show diagnostic cns publish
Subject: cisco.cns.device.diag_results
```

This example shows how to display the subscribed subject:

```
Router# show diagnostic cns subscribe
Subject: cisco.cns.device.diag_get_results
```

Related Commands

Command	Description
diagnostic cns	Configures the CNS diagnostics.

show diagnostic description module

To display a detailed description of a diagnostic test available on a module, use the **showdiagnosticdescriptionmodule**command in user EXEC or privileged EXEC mode.

show diagnostic description module {**slot** | **slot**/**subslot**} **test** {**all** | **test-id** | **test-name**}

Syntax Description

slot	Specifies a module by slot number.
slot/subslot	Specifies a submodule by slot number and subslot or bay within the module.
all	Displays descriptions of all available tests.
test-id	Test identification number. See the Usage Guidelines for a list of tests.
test-name	Test name. See the Usage Guidelines for a list of tests.

Command Default

This command has no default settings.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	This command was introduced for the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You can display detailed descriptions of diagnostic tests by specifying the test ID, the test name, or the **all**keyword in this command. The test ID and test name for available diagnostic tests are displayed in the output of the **showdiagnosticcontentmodule**command.

Examples

This example shows how to display the description of TestIPv6FibShortcut on module 1:

```
Router# show diagnostic description module 1 test TestIPv6FibShortcut
TestIPv6FibShortcut :
        This test verifies the IPv6 FIB forwarding of the layer 3 forwarding
        engine. One diagnostic IPv6 FIB and an adjacency entry are installed
        and a diagnostic IPv6 packet is sent to make sure it is forwarded
        accordingly based on rewritten MAC and VLAN information.
```

This example shows how to display the description of test number 15 on module 1:

```
Router# show diagnostic description module 1 test 15
TestIPv6FibShortcut :
        This test verifies the IPv6 FIB forwarding of the layer 3 forwarding
        engine. One diagnostic IPv6 FIB and an adjacency entry are installed
        and a diagnostic IPv6 packet is sent to make sure it is forwarded
        accordingly based on rewritten MAC and VLAN information.
```

Related Commands

Command	Description
show diagnostic content module	Displays the available diagnostic tests.

show diagnostic events

To display the diagnostic event log, use the **showdiagnosticevents**command in user EXEC or privileged EXEC mode.

show diagnostic events [{**event-type** *event-type* | **module** {**all***slotslot/subslot*}}]

Cisco ASR 1000 Series Aggregation Services Routers
show diagnostic events [{**event-type** *event-type* | **slot** {*number* | **all**}}]

Syntax Description

event-type *event-type*	(Optional) Displays events of a specified type, where *event-type* values are **error**, **info**, and **warning**.
module	(Optional) Displays the event log for a module, where: • **all** --Displays the event log for all modules. • *slot* --Chassis slot location of the module. • *slot* / *subslot* --Subslot or bay location of the submodule.
slot {*number* | **all**}	(Optional--Cisco ASR 1000 Series Routers) Displays the event log for the specified hardware slots, where: • *number* --Chassis slot location of the hardware, such as **R0** for route processor 0. • **all** --Displays the event log for hardware in all supported slots.

Command Default

When no optional keywords are specified, the **showdiagnosticevents** command displays all events for all hardware module or slot locations.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	This command was introduced for the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

If you do not enter a **module** keyword and argument for the **showdiagnosticevents** command, the event log for all modules is displayed.

On the Cisco ASR 1000 Series Aggregation Services Routers, if no optional keywords are entered, the event log for all supported slots is displayed.

The following fields are displayed in the command output:

Field	Description
Time Stamp	Date and time of the diagnostic event, in the format MM:DD hh:mm:ss.mss.
ET	Type of event (I=Info, W=Warning, E=Error).
Card	Module associated with the event.
Event Message	Event description.

Examples

The following example shows how to display the diagnostic event log for events of type Info:

```
Router# show diagnostic events event-type info
Diagnostic events (storage for 500 events, 14 events recorded)
Number of events matching above criteria = 10
Event Type (ET):I - Info, W - Warning, E - Error
Time Stamp         ET [Card] Event Message
------------------ --  -------------------------------------------------------
08/26 15:51:04.335 I  [1] TestIndexLearn Passed
08/26 15:51:04.335 I  [1] Diagnostics Passed
08/26 15:51:15.511 I  [8] TestLoopback Passed
08/26 15:51:15.511 I  [8] Diagnostics Passed
08/26 16:15:02.247 I  [1] TestDontLearn Passed
08/26 16:15:02.247 I  [1] Diagnostics Passed
08/26 16:15:12.683 I  [8] TestNetflowInlineRewrite Passed
08/26 16:15:12.683 I  [8] Diagnostics Passed
08/26 16:15:42.207 I  [2] TestActiveToStandbyLoopback Passed
08/26 16:15:42.207 I  [2] Diagnostics Passed
```

The following example shows the results of all events for the predefined TestErrorCounterMonitor test on route processor 0 on a Cisco ASR 1000 Aggregation Services Router:

```
Router# show diagnostic events slot R0

Diagnostic events (storage for 10 events, 10 events recorded)
Number of events matching above criteria = 10
Event Type (ET): I - Info, W - Warning, E - Error
Time Stamp         ET [Card] Event Message
------------------ -- ------ -------------------------------------------------
10/13 04:29:00.384 E  [R0]    TestErrorCounterMonitor Failed
10/13 04:29:05.501 E  [R0]    TestErrorCounterMonitor Failed
10/13 04:29:10.607 E  [R0]    TestErrorCounterMonitor Failed
10/13 04:29:15.730 E  [R0]    TestErrorCounterMonitor Failed
10/13 04:29:20.835 E  [R0]    TestErrorCounterMonitor Failed
10/13 04:29:25.939 E  [R0]    TestErrorCounterMonitor Failed
10/13 04:29:31.044 E  [R0]    TestErrorCounterMonitor Failed
10/13 04:29:36.149 E  [R0]    TestErrorCounterMonitor Failed
10/13 04:29:41.252 E  [R0]    TestErrorCounterMonitor Failed
10/13 04:29:46.356 E  [R0]    TestErrorCounterMonitor Failed
```

Related Commands

Command	Description
diagnostic event-log size	Modifies the diagnostic event log size dynamically.
diagnostic monitor	Configures the health-monitoring diagnostic testing.

Command	Description
diagnostic ondemand	Configures the on-demand diagnostics.
diagnostic schedule test	Sets the scheduling of test-based diagnostic testing for a specific module or schedule a supervisor engine switchover.
diagnostic start	Runs the specified diagnostic test.
diagnostic stop	Stops the testing process.

show diagnostic result slot

To display diagnostic test results for supported hardware slot locations, use the **showdiagnosticresultslot** command in privileged EXEC configuration mode.

show diagnostic result slot [{*number* [{**detail** | **failure** [**detail**] | **test** *testid* [**detail**] | **xml**}] | **all** [{**detail** | **failure** [**detail**]}]}]

Syntax Description

number	(Optional) Slot location of the hardware for which you want diagnostic test results, such as **R0** for route processor slot 0.
detail	(Optional) Displays additional detailed information for the specified diagnostic test.
failure	(Optional) Displays only failed diagnostic test results.
test *test-id*	(Optional) Displays diagnostic test results for one or more specific tests, where *test-id* is one of the following: • Name of a diagnostic test. • Number of a diagnostic test. • Range of diagnostic test numbers (startrange-endrange). • List of diagnostic test numbers or range of numbers, separated by commas. • **all** --Keyword specifying all diagnostic tests.
xml	(Optional) Displays diagnostic text results in Extensible Markup Language (XML) format.
all	(Optional) Displays diagnostic test results for all supported hardware locations.

Command Default

If you do not specify any options, the command displays diagnostic test results for all supported hardware slot locations.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.

Usage Guidelines

If a test does not exist for the hardware, "*Diagnostic is not available* " is shown.

In the command output, the possible testing results are as follows:

- Passed (.)
- Failed (F)
- Unknown (U)

Examples

The following example shows a passed diagnostic test (indicated by a ".") called TestErrorCounterMonitor on route processor slot 0, and no supported diagnostic tests on slot F0 and slot 0:

```
Router# show diagnostic result slot all
Current bootup diagnostic level: minimal
slot R0: ASR1000-RP1           SerialNo : JAE1218GSMR
  Overall Diagnostic Result for slot R0 : PASS
  Diagnostic level at card bootup: minimal
  Test results: (. = Pass, F = Fail, U = Untested)
    1) TestErrorCounterMonitor ---------> .
Diagnostic[slot F0]: Diagnostic is not available.
Diagnostic[slot 0]: Diagnostic is not available.
```

The following example shows detailed information about the diagnostic test on the hardware in slot R0:

```
Router# show diagnostic result slot R0 detail

Current bootup diagnostic level: minimal
slot R0: ASR1000-RP1           SerialNo : JAE1224L2QP
  Overall Diagnostic Result for slot R0 : PASS
  Diagnostic level at card bootup: minimal
  Test results: (. = Pass, F = Fail, U = Untested)
  ___________________________________________________________________________
    1) TestErrorCounterMonitor ---------> .
          Error code ------------------> 0 (DIAG_SUCCESS)
          Total run count -------------> 871
          Last test testing type ------> Health Monitoring
          Last test execution time ----> Oct 13 2009 03:15:47
          First test failure time -----> Oct 13 2009 02:02:32
          Last test failure time ------> Oct 13 2009 03:10:09
          Last test pass time ---------> Oct 13 2009 03:15:47
          Total failure count ---------> 10
          Consecutive failure count ---> 0
  ___________________________________________________________________________
```

show diagnostic simulation failure

To display a list of simulated test failures installed by the user for a module, use the **showdiagnosticsimulationfailure** command in user EXEC or privileged EXEC mode.

show diagnostic simulation failure [{**all** | **module** {**all***list slot* | *slot*/*subslot*}}]

Syntax Description

all	(Optional) Displays the diagnostic simulation failure for all modules.
module	(Optional) Specifies the module number.
list	A list of modules in the following format: • Entries are separated by a comma, for example, 1,4,6-10. • Ranges are specified with a hyphen, for example, 1-4,6-10.
slot	Specifies a single module by slot number.
slot / *subslot*	Specifies a single submodule by slot number and subslot or bay within the module.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	This command was implemented on the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If you do not enter a **module** keyword and argument for this command, information for all modules is displayed.

A diagnostic test configured for failure simulation is identified in the output of this command by its test ID number. You can use the **showdiagnosticdescriptionmodule**command to see the name and detailed description of a diagnostic test.

Examples

The following example shows how to display the simulated test failures installed by the user on module 1:

```
Router# show diagnostic simulation failure module 1
Module 1:
    Test #17: Simulation = Always Fail
```

Related Commands

Command	Description
show diagnostic description module	Describes the diagnostic tests.
test diagnostic simulation	Configures simulated diagnostic test conditions.

show diagnostic health

To display the output for the health checks performed, use the **showdiagnostichealth**command in user EXEC or privileged EXEC mode.

show diagnostic health

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.

Usage Guidelines

The command output displays the following system health check information:

- CPU and memory utilization
  - Displays warning if the CPU utilization in the last five minutes is greater than 70%
  - Displays total, free, and reserved memory statistics
- EARL recovery patch occurrences, shown as a log
- Nonzero ASIC error registers on all modules using the output listing of TestErrorCounterMonitor
- Nonzero port level error counters for all ports

Examples

This example shows how to display the output for the health checks performed:

```
Router# show diagnostic health
CPU utilization for the past 5 mins is greater than 70%
five minutes: 81%
EARL reset history:
Module 1 : WS-SUP32-GE-3B EARL patch log -
Num. of times patch applied   : 0
Num. of times patch requested : 0
Non-zero port counters for 1/8 -
13.                       linkChange = 338702
Non-zero port counters for 1/9 -
 0.                  rxCRCAlignErrors = 2
 3.                    rxFragmentPkts = 9
 6.                        ifInErrors = 30
13.                        linkChange = 1
Current bootup diagnostic level: minimal
Test results: (. = Pass, F = Fail, U = Untested)
36) TestErrorCounterMonitor ---------> F
Error code ------------------> 1 (DIAG_FAILURE)
Total run count -------------> 29
Last test execution time ----> Mar 16 2008 19:04:02
First test failure time -----> Mar 16 2008 19:03:21
Last test failure time ------> Mar 16 2008 19:04:02
```

```
Last test pass time ---------> Mar 16 2008 19:03:19
Total failure count ---------> 4
Consecutive failure count ---> 4
Error Records as following.
ID -- Asic Identification
IN -- Asic Instance
PO -- Asic Port Number
RE -- Register Identification
RM -- Register Identification More
EG -- Error Group
DV -- Delta Value
CF -- Consecutive Failure
TF -- Total Failure
ID IN PO RE RM DV EG CF TF
---------------------------------------------------------------
26 0 0 338 255 256 2 13 13
26 0 0 344 255 256 2 13 13
26 0 0 358 255 256 2 13 13
System Memory: 524288K total, 353225K used, 171063K free, 1000K kernel reserved
Lowest(b) : 171020288
Process kernel, type POSIX, PID = 1
0K total, 0K text, 0K data, 0K stack, 0K dynamic
Process sbin/chkptd.proc, type POSIX, PID = 16386
2296K total, 1988K text, 120K data, 12K stack, 176K dynamic
65536 heapsize, 55356 allocated, 8084 free
```

Related Commands

Command	Description
diagnostic monitor	Configures the health-monitoring diagnostic testing.

show diagnostic ondemand settings

To display the settings for the on-demand diagnostics, use the **showdiagnosticondemandsettings**command in user EXEC or privileged EXEC mode.

show diagnostic ondemand settings

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	This command was introduced for the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The command output shows the number of test iterations to be performed and the action to be taken on a test failure. Possible actions are:

- continue--Continue the ondemand tests until the test failure limit is reached.
- stop--Stop the ondemand tests immediately if a test fails.

Examples

This example shows how to display the settings for the on-demand diagnostics:

```
Router# show diagnostic ondemand settings
Test iterations = 1
Action on test failure = continue
```

Related Commands

Command	Description
diagnostic ondemand	Configures the on-demand diagnostics.

show diagnostic result module

To display the diagnostic test results for a module, use the **showdiagnosticresult**command in user EXEC or privileged EXEC mode.

show diagnostic result module {**all***listslot* | *slot* / *subslot*} [{**detail** | **failure** [**detail**] | **test** *test-id* [**detail**] | **xml**}]

Syntax Description

all	Displays diagnostic test results for all modules.
list	A list of modules in the following format: • Entries are separated by a comma, for example, 1,4,6-10. • Ranges are specified with a hyphen, for example, 1-4,6-10.
slot	Specifies a single module by slot number.
slot/subslot	Specifies a single submodule by slot number and subslot or bay within the module.
detail	(Optional) Displays the detailed test results.
failure	(Optional) Displays the failed test results.
test *test-id*	(Optional) Displays the test results only for the specified test. See the Usage Guidelines for a list of tests.
xml	(Optional) Displays the test results in XML form.

Command Default

This command has no default settings.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	This command was introduced for theSupervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

In the command output, the possible testing results are as follows:

- Passed (.)
- Failed (F)
- Unknown (U)

To display only the results of failed diagnostic tests, use the **failure**keyword.

To display the results of a specific diagnostic test, specify the *test-id* number using the **test***test-id*keyword and argument. The *test-id* numbers for available diagnostic tests are displayed in the output of the **showdiagnosticcontentmodule**command.

You can use the **showdiagnosticdescriptionmodule**command to see a detailed description of a diagnostic test.

Examples

This example shows how to display a summary of all diagnostic test results for the module in slot 3:

```
Router# show diagnostic result module 3
Current bootup diagnostic level:complete
Module 3:
  Overall Diagnostic Result for Module 8 :PASS
  Diagnostic level at card bootup:complete
  Test results:(. = Pass, F = Fail, U = Untested)
   1) TestLoopback :
      Port  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
      ----------------------------------------------------------------------------
            .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
      Port 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
      ----------------------------------------------------------------------------
            .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
   2) TestNewLearn --------------------> .
   3) TestIndexLearn ------------------> .
   4) TestDontLearn -------------------> .
   5) TestConditionalLearn ------------> .
   6) TestDontLearn -------------------> .
   7) TestConditionalLearn ------------> .
   8) TestBadBpdu ---------------------> .
   9) TestTrap ------------------------> .
  10) TestMatch -----------------------> .
  11) TestCapture ---------------------> .
  12) TestProtocolMatch ---------------> .
  13) TestChannel ---------------------> .
  14) TestIPFibShortcut ---------------> .
  15) TestDontShortcut ----------------> .
  16) TestL3Capture2 ------------------> .
  17) TestL3VlanMet -------------------> .
  18) TestIngressSpan -----------------> .
  19) TestEgressSpan ------------------> .
  20) TestAclPermit -------------------> .
  21) TestAclDeny ---------------------> .
  22) TestNetflowInlineRewrite:
      Port  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
      ----------------------------------------------------------------------------
            .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
      Port 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
      ----------------------------------------------------------------------------
            .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
```

This example shows how to display the detailed test results for the module in slot 1:

```
Router# show diagnostic result module 1 detail
Current bootup diagnostic level:complete
Module 1:
  Overall Diagnostic Result for Module 1 :PASS
  Diagnostic level at card bootup:complete
  Test results:(. = Pass, F = Fail, U = Untested)
___________________________________________________________________________
   1) TestDummy -----------------------> .
```

```
          Error code ------------------> 0 (DIAG_SUCCESS)
          Total run count -------------> 90
          Last test execution time ----> Dec 10 2002 12:34:30
          First test failure time -----> Dec 10 2002 11:57:39
          Last test failure time ------> Dec 10 2002 12:34:10
          Last test pass time ---------> Dec 10 2002 11:34:30
          Total failure count ---------> 65
          Consecutive failure count ---> 0
___________________________________________________________________________
 2) TestLoopback:
      Port  1  2
      ----------
            .  .
          Error code ------------------> 0 (DIAG_SUCCESS)
          Total run count -------------> 1
          Last test execution time ----> Dec 10 2002 12:37:18
          First test failure time -----> n/a
          Last test failure time ------> n/a
          Last test pass time ---------> Dec 10 2002 12:37:18
          Total failure count ---------> 0
          Consecutive failure count ---> 0
.
.
.
[...continues...]
```

Related Commands

Command	Description
show diagnostic content module	Displays the available diagnostic tests.
show diagnostic description module	Describes the diagnostic tests.

show diagnostic sanity

To display sanity check results, use the **show diagnostic sanity** command in privileged EXEC mode.

show diagnostic sanity

Syntax Description

This command has no arguments or keywords.

Command Default

Displays information for all the Gigabit Ethernet WAN interfaces in the Cisco 7600 series router.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The sanity check runs a set of predetermined checks on the configuration with a possible combination of certain system states to compile a list of warning conditions. The checks are designed to look for anything that seems out of place and are intended to serve as an aid to maintaining the system sanity.

The following is a list of the checks that are run and the action taken when the condition is found:

- Checks whether the default gateways are reachable. If so, the system stops pinging.
- If a port auto-negotiates to half duplex, the system flags it.

Trunking Checks

- If a trunk port has the mode set to “on,” the system flags it.
- If a port is trunking and mode is auto, the system flags it.
- If a trunk port is not trunking and the mode is desirable, the system flags it.
- If a trunk port negotiates to half duplex, the system flags it.

Channeling Checks

- If a port has channeling mode set to on, the system flags it.
- If a port is not channeling and the mode is set to desirable, the system flags it.
- If a VLAN has a Spanning-Tree root of 32K (root is not set), the system flags it.

Spanning-Tree VLAN Checks

- If a VLAN has a max age on the Spanning-Tree root that is different than the default, the system flags it.
- If a VLAN has a fwd delay on the Spanning-Tree root that is different than the default, the system flags it.
- If a VLAN has a fwd delay on the bridge that is different than the default, the system flags it.

- If a VLAN has a fwd delay on the bridge that is different than the default, the system flags it.
- If a VLAN has a hello time on the bridge that is different than the default, the system flags it.

Spanning-Tree Port Checks

- If a port has a port cost that is different than the default, the system flags it.
- If a port has a port priority that is different than the default, the system flags it.

UDLD Checks

- If a port has UDLD disabled, the system flags it.
- If a port had UDLD shut down, the system flags it.
- If a port had a UDLD undetermined state, the system flags it.

Assorted Port Checks

- If a port had receive flow control disabled, the system flags it.
- If a trunk port had PortFast enabled, the system flags it.
- If a inline power port has any of the following states:
    - denied
    - faulty
    - other
    - off

The system flags it.

- If a port has a native VLAN mismatch, the system flags it.
- If a port has a duplex mismatch, the system flags it.

Bootstring and Config Register Checks

- The config register on the primary supervisor engine (and on the secondary supervisor engine if present) must be one of the following values: 0x2 , 0x102, or 0x2102.
- The system verifies the bootstring on the primary supervisor engine (and on the secondary supervisor engine if present). The system displays a message if the bootstring is empty.
- The system verifies that every file is specified in the bootstring. The system displays a message if the file is absent or shows up with a wrong checksum.

If only *device* **:** is specified as a filename, then the system verifies that the first file is on the device.

Assorted Checks

- The system displays a message if IGMP snooping is disabled.
- The system displays a message if any of the values of the snmp community access strings {RO,RW,RW-ALL} is the same as the default.
- The system displays a message if any of the modules are in states other than “Ok.”

- The system displays a message that lists all the tests that failed (displayed as an “F”) in the **show test all** command.
- The system displays a message if *fast is not configured on the switch anywhere.
- The system displays a message if there is enough room for the crashinfo file on the bootflash:.
- The system displays a message if multicast routing is enabled globally but is not applied to all interfaces.
- The system displays a message if IGMP snooping is disabled and RGMP is enabled.

Examples

This example displays samples of the messages that could be displayed with the **show diagnostic sanity** command:

```
Router# show diagnostic sanity
Pinging default gateway 10.6.141.1 ....
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.6.141.1, timeout is 2 seconds:
..!!.
Success rate is 0 percent (0/5)
IGMP snooping disabled please enable it for optimum config.
IGMP snooping disabled but RGMP enabled on the following interfaces,
please enable IGMP for proper config :
Vlan1, Vlan2, GigabitEthernet1/1
Multicast routing is enabled globally but not enabled on the following
interfaces:
GigabitEthernet1/1, GigabitEthernet1/2
A programming algorithm mismatch was found on the device bootflash:
Formatting the device is recommended.
The bootflash: does not have enough free space to accomodate the crashinfo file.
Please check your confreg value : 0x0.
Please check your confreg value on standby: 0x0.
The boot string is empty. Please enter a valid boot string .
Could not verify boot image "disk0:" specified in the boot string on the
slave.
Invalid boot image "bootflash:asdasd" specified in the boot string on the
slave.
Please check your boot string on the slave.
UDLD has been disabled globally - port-level UDLD sanity checks are
being bypassed.
OR
[
The following ports have UDLD disabled. Please enable UDLD for optimum
config:
Fa9/45
The following ports have an unknown UDLD link state. Please enable UDLD
on both sides of the link:
Fa9/45
]
The following ports have portfast enabled:
Fa9/35, Fa9/45
The following ports have trunk mode set to on:
Fa4/1, Fa4/13
The following trunks have mode set to auto:
Fa4/2, Fa4/3
The following ports with mode set to desirable are not trunking:
Fa4/3, Fa4/4
The following trunk ports have negotiated to half-duplex:
Fa4/3, Fa4/4
The following ports are configured for channel mode on:
Fa4/1, Fa4/2, Fa4/3, Fa4/4
```

```
The following ports, not channeling are configured for channel mode
desirable:
Fa4/14
The following vlan(s) have a spanning tree root of 32768:
1
The following vlan(s) have max age on the spanning tree root different from
the default:
1-2
The following vlan(s) have forward delay on the spanning tree root different
from the default:
1-2
The following vlan(s) have hello time on the spanning tree root different
from the default:
1-2
The following vlan(s) have max age on the bridge different from the
default:
1-2
The following vlan(s) have fwd delay on the bridge different from the
default:
1-2
The following vlan(s) have hello time on the bridge different from the
default:
1-2
The following vlan(s) have a different port priority than the default
on the port FastEthernet4/1
1-2
The following ports have recieve flow control disabled:
Fa9/35, Fa9/45
The following inline power ports have power-deny/faulty status:
Gi7/1, Gi7/2
The following ports have negotiated to half-duplex:
Fa9/45
The following vlans have a duplex mismatch:
Fas 9/45

The following interafaces have a native vlan mismatch:
interface (native vlan - neighbor vlan)
 Fas 9/45 (1 - 64)
The value for Community-Access on read-only operations for SNMP is the same
as default. Please verify that this is the best value from a security point
of view.
The value for Community-Access on write-only operations for SNMP is the same
as default. Please verify that this is the best value from a security point
of view.
The value for Community-Access on read-write operations for SNMP is the same
as default. Please verify that this is the best value from a security point
of view.
Please check the status of the following modules:
8,9
Module 2 had a MINOR_ERROR.
The Module 2 failed the following tests:
TestIngressSpan
The following ports from Module2 failed test1:
1,2,4,48
```

show diagnostic schedule module

To display the current scheduled diagnostic tasks, use the **showdiagnosticschedulemodule**command in user EXEC or privileged EXEC mode.

show diagnostic schedule module {**all***listslot* | *slot* / *subslot*}

Syntax Description

all	Displays the current scheduled diagnostic tasks for all modules.
list	A list of modules in the following format: • Entries are separated by a comma, for example, 1,4,6-10. • Ranges are specified with a hyphen, for example, 1-4,6-10.
slot	Specifies a single module by slot number.
slot/subslot	Specifies a single submodule by slot number and subslot or bay within the module.

Command Default

This command has no default settings.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	This command was introduced for the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

A scheduled diagnostic test is identified in the output of this command by its test ID number. With the test ID number, you can see the name and detailed description of the diagnostic test by using the **showdiagnosticdescriptionmodule**command.

Examples

This example shows how to display the current scheduled diagnostic tasks for the module in slot 1:

```
Router# show diagnostic schedule module 1
Current Time = 07:55:30 UTC Fri August 2 2002
Diagnostic for Module 1:
Schedule #1:
        To be run on January 3 2003 23:32
        Test ID(s) to be executed:1.
Schedule #2:
        To be run daily 14:45
        Test ID(s) to be executed:2.
Schedule #3:
        To be run weekly Monday 3:33
        Test ID(s) to be executed:all.
```

Related Commands

Command	Description
diagnostic schedule test	Sets the scheduling of test-based diagnostic testing for a specific module or schedule a supervisor engine switchover.
show diagnostic description module	Describes the diagnostic tests.

show diagnostic status

To display the currently running diagnostics tests, use the **showdiagnosticstatus**command in user EXEC or privileged EXEC mode.

show diagnostic status

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	This command was introduced for the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

For each installed module, the following fields are displayed in the command output:

Field	Description
Card	The slot number of the module associated with the event
Description	A description of the module
Current Running Test	The diagnostic test running on the module
Run by	The diagnostic test category that initiated the running test. The categories are: • BU--This test is running as a part of the bootup diagnostics • HM--This test is running as a part of the health monitoring diagnostics • OD--This was initiated as an ondemand diagnostic test • SCH--This test is running as a scheduled diagnostic test

Examples

This example shows how to display the currently running diagnostics tests:

```
Router# show diagnostic status
<BU> - Bootup Diagnostics, <HM> - Health Monitoring Diagnostics, <OD> - OnDemand Diagnostics,
 <SCH> - Scheduled Diagnostics
====== ================================= =============================== ======
Card   Description                       Current Running Test            Run by
------ --------------------------------- ------------------------------- ------
3      CEF720 48 port 10/100/1000mb Ethe TestLoopback                    <OD>
5      Supervisor Engine 720 (Hot)       TestScratchRegister             <HM>
6      Supervisor Engine 720 (Active)    N/A                             N/A
```

```
8      CEF720 8 port 10GE with DFC       N/A                              N/A
====== ================================= ================================ ======
```

Related Commands

Command	Description
diagnostic start	Runs the specified diagnostic test.
diagnostic stop	Stops the testing process.
show diagnostic content module	Displays the available diagnostic tests.
show diagnostic description module	Describes the diagnostic tests.

show dsc clock

To display information about the dial shelf controller clock, use the **showdscclock**command in privileged EXEC mode with the line card execute (**execute-on**) command.

execute-on {**slot** *slot-number* | **all**} **show dsc clock**

Syntax Description

execute-on	Executes commands remotely on a line card.
slot *slot-number*	Displays information for a specific slot. Slot number (12 or 13) must be occupied by a DSC card.
all	Executes the command on all line cards.

Command Modes

EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You must use the **showdscclock** command from the router using the **execute-on** command.

Examples

The following is sample output from the **showdscclock** command:

```
Router# execute-on slot 12
 show dsc clock
Router#
Primary Clock:
--------------
Slot: 3, Port 1, Line 0, Priority = 3 up since 00:37:56
Time elapsed since last failure of the primary = 00:38:59

Backup clocks:
Source  Slot    Port    Line    Priority    Status      State
--------------------------------------------------------------
Trunk   1       2       0       10          Good        Configured

All feature boards present are getting good clock from DSC
```

The table below describes the significant fields shown in the display.

Table 100: show dcs clock Field Descriptions

Field	Description
Primary clock	The clock designated as the master timing clock.

Field	Description
Priority	The order in which a clock is designated to back up the primary clock or the next higher priority clock in case of its failure.
Backup Source	The clock signal source, such as a trunk, internal clock, or external generator.
Feature board	An application-specific card in the dial shelf, such as a line card.
Trunk	The trunk line connected to the ISP or central office.
Status	Whether the clock source is capable of providing a synch source signal.
State	Whether the clock source is connected and assigned a priority.

Related Commands

Command	Description
execute-on	Executes commands remotely on a line card.

show dsi

To display information about the dial shelf interconnect (DSI) port adapter parameters, use the **showdsi** command in privileged EXEC mode with the line card execute (**execute-on**) command.

execute-on {**slot** *slot-number* | **all**} **show dsi**

Syntax Description

execute-on	Executes commands remotely on a line card.
slot *slot-number*	Displays information for a specific slot. Slot number (12 or 13) must be occupied by a DSC card.
all	Executes the command on all line cards.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The dial shelf interconnect (DSI) port adapter connects the Cisco 5814 dial shelf to the Cisco 7206 router shelf. The DSI port adapter allows data transfers between the dial shelf and the router shelf. Data is converted into packets by the feature cards, transmitted to a hub on the dial shelf controller card, and from there sent to the router shelf. Conversely, packets from the router shelf are sent to the dial shelf controller card, where they are transmitted over the backplane to the modem and trunk cards. The show dsi command is used to show information about the dial shelf interconnect hardware, interface, physical link, PCI registers, and address filters.

Examples

The following is sample output from the **showdsi**command:

```
Router# execute-on slot 1 show dsi
DSI-Tx-FastEthernet0 is up, line protocol is up
  Hardware is DEC21140A, address is 0008.26b7.b008 (bia 0008.26b7.b008)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  Half-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 01:17:09, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     6 packets input, 596 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast
```

```
     0 input packets with dribble condition detected
     6170 packets output, 813483 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
DSI-Rx-FastEthernet1 is up, line protocol is up
Hardware is DEC21140A, address is 0008.26b7.b008 (bia 0008.26b7.b008)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     6280 packets input, 362493 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Interface DSI-Tx-FastEthernet0
Hardware is DEC21140A
 dec21140_ds=0x604C9FC4, registers=0x3C000000, ib=0x1912E00
 rx ring entries=128, tx ring entries=256
 rxring=0x1912F00, rxr shadow=0x604CA16C, rx_head=6, rx_tail=0
 txring=0x1913740, txr shadow=0x604CA398, tx_head=138, tx_tail=138, tx_count=0
 PHY link up
 CSR0=0xFE024882, CSR3=0x1912F00, CSR4=0x1913740, CSR5=0xFC660000
 CSR6=0x320CA002, CSR7=0xFFFFA261, CSR8=0xE0000000, CSR9=0xFFFDC3FF
 CSR11=0xFFFE0000, CSR12=0xFFFFFF09, CSR15=0xFFFFFEC8
 DEC21140 PCI registers:
  bus_no=0, device_no=1
  CFID=0x00091011, CFCS=0x02800006, CFRV=0x02000022, CFLT=0x0000FF00
  CBIO=0x00000001, CBMA=0x48000000, CFIT=0x28140100, CFDA=0x00000000
 MII registers:
  Register 0x00:   FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF
  Register 0x08:   FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF
  Register 0x10:   FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF
  Register 0x18:   FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF
 throttled=0, enabled=0, disabled=0
 rx_fifo_overflow=0, rx_no_enp=0, rx_discard=0
 tx_underrun_err=0, tx_jabber_timeout=0, tx_carrier_loss=0
 tx_no_carrier=0, tx_late_collision=0, tx_excess_coll=0
 tx_collision_cnt=0, tx_deferred=0, fatal_tx_err=0, tbl_overflow=0
 HW addr filter: 0x604CABC4, ISL Disabled
  Entry= 0:  Addr=FFFF.FFFF.FFFF
  Entry= 1:  Addr=FFFF.FFFF.FFFF
  Entry= 2:  Addr=FFFF.FFFF.FFFF
  Entry= 3:  Addr=FFFF.FFFF.FFFF
  Entry= 4:  Addr=FFFF.FFFF.FFFF
  Entry= 5:  Addr=FFFF.FFFF.FFFF
  Entry= 6:  Addr=FFFF.FFFF.FFFF
  Entry= 7:  Addr=FFFF.FFFF.FFFF
  Entry= 8:  Addr=FFFF.FFFF.FFFF
  Entry= 9:  Addr=FFFF.FFFF.FFFF
  Entry=10:  Addr=FFFF.FFFF.FFFF
```

```
  Entry=11:  Addr=FFFF.FFFF.FFFF
  Entry=12:  Addr=FFFF.FFFF.FFFF
  Entry=13:  Addr=FFFF.FFFF.FFFF
  Entry=14:  Addr=FFFF.FFFF.FFFF
  Entry=15:  Addr=0008.26B7.B008

Interface DSI-Rx-FastEthernet1
Hardware is DEC21140A
dec21140_ds=0x604DDA4C, registers=0x3C000800, ib=0x1A01FC0
rx ring entries=128, tx ring entries=256
 rxring=0x1A020C0, rxr shadow=0x604DDBF4, rx_head=55, rx_tail=0
 txring=0x1A02900, txr shadow=0x604DDE20, tx_head=2, tx_tail=2, tx_count=0
 PHY link up
 CSR0=0xFE024882, CSR3=0x1A020C0, CSR4=0x1A02900, CSR5=0xFC660000
 CSR6=0x320CA202, CSR7=0xFFFFA261, CSR8=0xE0000000, CSR9=0xFFFDC3FF
 CSR11=0xFFFE0000, CSR12=0xFFFFFF09, CSR15=0xFFFFFEC8
 DEC21140 PCI registers:
  bus_no=0, device_no=2
  CFID=0x00091011, CFCS=0x02800006, CFRV=0x02000022, CFLT=0x0000FF00
  CBIO=0x00000001, CBMA=0x48000800, CFIT=0x28140100, CFDA=0x00000000
 MII registers:
  Register 0x00:   FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF
  Register 0x08:   FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF
  Register 0x10:   FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF
  Register 0x18:   FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF
 throttled=0, enabled=0, disabled=0
 rx_fifo_overflow=0, rx_no_enp=0, rx_discard=0
 tx_underrun_err=0, tx_jabber_timeout=0, tx_carrier_loss=0
 tx_no_carrier=0, tx_late_collision=0, tx_excess_coll=0
 tx_collision_cnt=0, tx_deferred=0, fatal_tx_err=0, tbl_overflow=0
 HW addr filter: 0x604DE64C, ISL Disabled
  Entry= 0:  Addr=FFFF.FFFF.FFFF
  Entry= 1:  Addr=FFFF.FFFF.FFFF
  Entry= 2:  Addr=FFFF.FFFF.FFFF
  Entry= 3:  Addr=FFFF.FFFF.FFFF
  Entry= 4:  Addr=FFFF.FFFF.FFFF
  Entry= 5:  Addr=FFFF.FFFF.FFFF
  Entry= 6:  Addr=FFFF.FFFF.FFFF
  Entry= 7:  Addr=FFFF.FFFF.FFFF
  Entry= 8:  Addr=FFFF.FFFF.FFFF
  Entry= 9:  Addr=FFFF.FFFF.FFFF
  Entry=10:  Addr=FFFF.FFFF.FFFF
  Entry=11:  Addr=FFFF.FFFF.FFFF
  Entry=12:  Addr=FFFF.FFFF.FFFF
  Entry=13:  Addr=FFFF.FFFF.FFFF
  Entry=14:  Addr=FFFF.FFFF.FFFF
  Entry=15:  Addr=0008.26B7.B008
```

The table below describes the significant fields shown in the display.

Table 101: show dsi Field Descriptions

Field	Description
FastEthernet0 ... is up ... is administratively down	Indicates whether the interface hardware is currently active and if it has been taken down by an administrator.
line protocol is	Indicates whether the software processes that handle the line protocol consider the line usable or if it has been taken down by an administrator.
Hardware	Hardware type (for example, MCI Ethernet, SCI,[2] CBus[3] Ethernet) and address.

Field	Description
Internet address	Internet address followed by subnet mask.
MTU	Maximum Transmission Unit of the interface.
BW	Bandwidth of the interface in kilobits per second.
DLY	Delay of the interface in microseconds.
rely	Reliability of the interface as a fraction of 255 (255/255 is 100% reliability), calculated as an exponential average over 5 minutes.
load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method assigned to interface.
ARP type:	Type of Address Resolution Protocol assigned.
loopback	Indicates whether loopback is set or not.
keepalive	Indicates whether keepalives are set or not.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface. Useful for knowing when a dead interface failed.
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by the interface. Useful for knowing when a dead interface failed.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the “last” fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. *** indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 231ms (and less than 232ms) ago.
Output queue, input queue, drops	Number of packets in output and input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped due to a full queue.
5 minute input rate, 5 minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic it sends and receives (rather than all network traffic). The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.

Field	Description
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernets and bursts of noise on serial lines are often responsible for no input buffer events.
Received ... broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the medium's minimum packet size. For instance, any Ethernet packet that is less than 64 bytes is considered a runt.
giants	Number of packets that are discarded because they exceed the medium's maximum packet size. For example, any Ethernet packet that is greater than 1518 bytes is considered a giant.
input errors	Includes runts, giants, no buffer, CRC, frame, overrun, and ignored counts. Other input-related errors can also cause the input errors count to be increased, and some datagrams may have more than one error; therefore, this sum may not balance with the sum of enumerated input error counts.
CRC	Cyclic redundancy checksum generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a LAN, this is usually the result of collisions or a malfunctioning Ethernet device.
overrun	Number of times the receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be increased.
abort	Number of packets whose receipt was aborted.
watchdog	Number of times watchdog receive timer expired. It happens when receiving a packet with length greater than 2048.
multicast	Number of multicast packets received.

Field	Description
input packets with dribble condition detected	Dribble bit error indicates that a frame is slightly too long. This frame error counter is incremented just for informational purposes; the router accepts the frame.
packets output	Total number of messages transmitted by the system.
bytes	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the transmitter has been running faster than the router can handle. This may never be reported on some interfaces.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors, as some datagrams may have more than one error, and others may have errors that do not fall into any of the specifically tabulated categories.
collisions	Number of messages retransmitted due to an Ethernet collision. This is usually the result of an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). A packet that collides is counted only once in output packets.
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within several seconds. On a serial line, this can be caused by a malfunctioning modem that is not supplying the transmit clock signal, or by a cable problem. If the system notices that the carrier detect line of a serial interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an interface is looped back or shut down.
restarts	Number of times a Type 2 Ethernet controller was restarted because of errors.
babbles	The transmit jabber timer expired.
late collision	Number of late collisions. Late collision happens when a collision occurs after transmitting the preamble.
deferred	Deferred indicates that the chip had to defer while ready to transmit a frame because the carrier was asserted.
lost carrier	Number of times the carrier was lost during transmission.
no carrier	Number of times the carrier was not present during the transmission.
output buffer failures	Number of failed buffers and number of buffers swapped out.

[2] SCI = Single Cell Input
[3] CBus = Command Bus

Command	Description
execute-on	Executes commands on a line card.
show dsip	Displays all information about the DSIP.
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

show dsip

To display all information about the Distributed System Interconnect Protocol (DSIP) on a Cisco AS5800, use the **showdsip**command in EXEC mode.

show dsip

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Your Cisco AS5800 universal access server uses a protocol used by the Cisco 7206 router shelf to communicate back and forth with the Cisco 5814 dial shelf controller card(s) and feature cards. Although dial shelf interconnect (DSI) configuration is transparent to the user, there are several show commands to help you view your setup, and debug commands to help you troubleshoot your system.

To display a subset of this information, use the**showdsipclients**, **showdsipnodes**, **showdsipports**, **showdsipqueue**,**showdsiptracing**, **showdsiptransport**, and **showdsipversion** commands.

Examples

The following is sample output from the **showdsip**command. For a description of the fields shown in the sample output, refer to the individual **showdsip**commands listed in the “Usage Guidelines” section.

```
Router# show dsip

DSIP Transport Statistics:
 IPC : input msgs=8233, bytes=699488; output msgs=8233, bytes=483558
        total consumed ipc msgs=682;  total freed ipc msgs = 682
        transmit contexts in use = 11, free = 245, zombie = 0, invalid = 0
        ipc getmsg failures = 0, ipc timeouts=0
        core getbuffer failures=0, api getbuffer failures=0
 dsip test msgs rcvd = 2770, sent = 0
 CNTL: input msgs=1112, bytes=91272; output msgs=146, bytes=8760
        getbuffer failures=0
 DATA: input msgs=0, bytes=0; output msgs=426, bytes=5112

DSIP Private  Buffer Pool Hits  = 0

DSIP Registered Addresses:
 Shelf0 : Master: 00e0.b093.2238, Status=local
 Shelf1 : Slot1 : 0007.5387.4808, Status=remote
 Shelf1 : Slot5 : 0007.5387.4828, Status=remote
 Shelf1 : Slot6 : 0007.5387.4830, Status=remote
 Shelf1 : Slot7 : 0007.5387.4838, Status=remote
```

```
 Shelf1 : Slot8 : 0007.5387.4840, Status=remote
 Shelf1 : Slot9 : 0007.5387.4848, Status=remote
 Shelf1 : Slot11: 0007.5387.4858, Status=remote
 Shelf1 : Slot12: 0007.4b67.8260, Status=remote
DSIP Clients:
-------------
ID    Name
0   Console
1   Clock
2   Modem
3   Logger
4   Trunk
5   Async data
6   TDM
7   Dial shelf manager
8   Environment Mon
9   DSIP Test
Dsip Local Ports:
----------------
Client:Portname             Portid    In-Msgs   Bytes     Last-i/p
Console:Master              10004     0         0         never
Clock:Master                10005     29        3464      00:00:40
Modem:Master                10006     90        70162     00:23:44
Logger:Master               10007     0         0         never
Trunk:Master                10008     1765      140480    00:00:08
Async data:Master           10009     0         0         never
TDM:Master                  1000A     7         112       00:24:19
Dial shelf manager:Master   1000B     28        4752      00:00:36
DSIP Test:Master            1000C     2922      2922      00:00:00

Dsip Remote Ports:
-----------------
Client:Portname             Portid    Out-Msgs  Bytes     Last-o/p  Last-act
Clock:Slave1                101005F   1         24        00:24:21  00:24:21
Trunk:Slave1                1010061   12        1776      00:24:21  00:24:21
Modem:Slave5                1050050   96        2148      00:23:56  00:24:19
Modem:Slave6                1060050   105       2040      00:24:00  00:24:22
Modem:Slave7                1070050   106       2188      00:23:56  00:24:20
Modem:Slave8                1080050   112       2212      00:24:13  00:24:35
Modem:Slave9                1090050   115       2224      00:24:09  00:24:35
Modem:Slave11               10B0050   107       2192      00:24:09  00:24:32
Clock:Slave12               10C000D   1         24        00:24:37  00:24:37
Dial shelf manager:Slave12  10C000E   28        4752      00:00:49  00:24:35
DSIP Test:Slave12           10C000F   0         0         never     00:24:35

DSIP ipc queue:
---------------
There are 0 IPC messages waiting for acknowledgement in the transmit queue.
There are 0 messages currently in use by the system.

DSIP ipc seats:
---------------
There are 9 nodes in this IPC realm.
   ID     Type                 Name                       Last  Last
                                                          Sent  Heard
   10000 Local       IPC Master                               0      0
 1060000 DSIP        Seat:Slave6                              10     10
 10C0000 DSIP        Seat:Slave12                             2963   13
 1080000 DSIP        Seat:Slave8                              10     10
 1090000 DSIP        Seat:Slave9                              10     10
 1010000 DSIP        Seat:Slave1                              16     16
 1070000 DSIP        Seat:Slave7                              10     10
 10B0000 DSIP        Seat:Slave11                             10     10
 1050000 DSIP        Seat:Slave5                              10     10
```

```
DSIP version information:
------------------------
Local DSIP major version =  3,    minor version = 2

All DS slots are running DSIP versions compatible with RS
Local Clients Registered Versions:
------------------------------------
Client Name      Major Version   Minor Version
Console          3               2
Clock            1               1
Modem            0               0
Logger           No version      No version
Trunk            No version      No version
Async data       No version      No version
TDM              No version      No version
DSIP Test        No version      No version

Mismatched  Remote Client Versions:
-----------------------------------
```

Related Commands

Command	Description
show dsip clients	Lists the clients registered with DSIP on a system.
show dsip nodes	Displays information about the processors running the DSIP.
show dsip ports	Displays information about local and remote ports.
show dsip queue	Displays the number of messages in the retransmit queue waiting for acknowledgment.
show dsip tracing	Displays DSIP tracing buffer information.
show dsip transport	Displays information about the DSIP transport statistics for the control/data and IPC packets and registered addresses.
show dsip version	Displays DSIP version information.
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

show dsip clients

To display information about Distributed System Interconnect Protocol (DSIP) clients, use the **showdsipclients**command in EXEC mode.

show dsip clients

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to see whether a client is actually registered with DSIP and using its services.

Consider the following example: a client “Trunk” seems to be defunct on a particular node with absolutely no input/output activity. The command show dsip ports does not show any Trunk port among its local ports though all other client ports show up. The problem might be that the Trunk client did not even register with DSIP. To confirm this, use the show dsip clients command.

Examples

The following is sample output from the **showdsipclients**command. This command lists the clients.

```
Router# show dsip clients
ID    Name
0   Console
1   Clock
2   Modem
3   Logger
4   Trunk
5   Async data
6   TDM
7   Dial shelf manager
8   Environment Mon
9   DSIP Test
```

Related Commands

Command	Description
show dsip nodes	Displays information about the processors running the DSIP.
show dsip ports	Displays information about local and remote ports
show dsip queue	Displays the number of messages in the retransmit queue waiting for acknowledgment.

Command	Description
show dsip tracing	Displays DSIP tracing buffer information.
show dsip transport	Displays information about the DSIP transport statistics for the control/data and IPC packets and registered addresses.
show dsip version	Displays DSIP version information.

show dsip nodes

To display information about the processors running the Distributed System Interconnect Protocol (DSIP), use the **showdsipnodes**command in EXEC mode.

show dsip nodes

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use show dsip nodes to see the nodes (slots) connected by DSIP and the node specific sequence numbers. The former information is also available from show dsip transport. The sequence numbers are useful for support engineers while debugging a problem.

Examples

The following is sample output from the **showdsipnodes** command:

```
Router# show dsip nodes

DSIP ipc nodes:
---------------
There are 9 nodes in this IPC realm.
   ID     Type                 Name                       Last  Last
                                                          Sent  Heard
   10000 Local      IPC Master                               0      0
 1130000 DSIP       Dial Shelf:Slave12                      12     12
 1080000 DSIP       Dial Shelf:Slave1                        1      1
 10A0000 DSIP       Dial Shelf:Slave3                        1      1
 10C0000 DSIP       Dial Shelf:Slave5                        1      1
 10D0000 DSIP       Dial Shelf:Slave6                        1      1
 10E0000 DSIP       Dial Shelf:Slave7                        1      1
 10F0000 DSIP       Dial Shelf:Slave8                        1      1
 1100000 DSIP       Dial Shelf:Slave9                        1      1
```

The table below describes the significant fields shown in the display.

Table 102: show dsip nodes Field Descriptions

Field	Description
ID	DSIP uses Cisco’s IPC (Inter Process Communication) module for nondata related (client control messages etc.) traffic. A seat or node is a computational element, such as a processor, that can be communicated with using IPC services. A seat is where entities and IPC ports reside. The IPC maintains a seat table which contains the seatids of all the seats in the system. Normally this seatid is a function of the slot number.
Type	Local: Local node. DSIP: Remote DSIP node.
Name	Each seat (node) has a name to easily identify it. There is only one primary node and rest are subordinate nodes. The master node name is “IPC Master” and the slave node name is “Seat:Slave X”, where “X” is the slot number of the node.
Last Sent/Last Heard	Each node maintains two sequence numbers for the last sent and last heard.
Last Sent	Whenever a message is sent out, the “last sent” counter is updated.
Last Heard	Whenever a message is received from a remote node, “last heard” is updated.

Related Commands

Command	Description
show dsip clients	Lists the clients registered with DSIP on a system.
show dsip ports	Displays information about local and remote ports
show dsip queue	Displays the number of messages in the retransmit queue waiting for acknowledgment.
show dsip tracing	Displays DSIP tracing buffer information.
show dsip transport	Displays information about the DSIP transport statistics for the control/data and IPC packets and registered addresses.
show dsip version	Displays DSIP version information.

show dsip ports

To display information about local and remote ports, use the **showdsipports**command in EXEC mode.

show dsip ports [{**local** | **remote** [**slot**]}]

Syntax Description

local	(Optional) Displays information for local ports. The local port is the port created at a seat's local end.
remote	(Optional) Displays information for remote ports. The remote port is the port residing on a remote seat to which DSIP IPC based connection is open.
slot	(Optional) Specifies a slot number to display information for a specific card on the dial shelf.

Command Modes

EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The DSIP communication going through the IPC stack uses ports. The creation of a port returns a 32-bit port ID which is the endpoint for communication between two IPC clients.

The show dsip ports command is used to check clients that are up and running:

- To see the local ports that are created and the activity on them.
- To see the remote ports which are connected and to see the activity on them.

If no options are specified, information is displayed for both local and remote ports.

Examples

The following is sample output from the **showdsipports** command:

```
Router# show dsip ports

Dsip Local Ports:
----------------
Client:Portname             Portid    In-Msgs   Bytes     Last-i/p
Console:Master              10004     0         0         never
Clock:Master                10005     16        1800      00:00:05
Modem:Master                10006     90        70162     00:10:08
Logger:Master               10007     0         0         never
Trunk:Master                10008     792       62640     00:00:03
Async data:Master           10009     0         0         never
TDM:Master                  1000A     7         112       00:10:44
Dial shelf manager:Master   1000B     15        2256      00:00:27
DSIP Test:Master            1000C     1294      1294      00:00:00
```

```
Dsip Remote Ports:
-----------------
Client:Portname             Portid    Out-Msgs  Bytes     Last-o/p  Last-act
Clock:Slave1                101005F   1         24        00:10:46  00:10:46
Trunk:Slave1                1010061   12        1776      00:10:46  00:10:46
Modem:Slave5                1050050   96        2148      00:10:21  00:10:44
Modem:Slave6                1060050   105       2040      00:10:25  00:10:48
Modem:Slave7                1070050   106       2188      00:10:21  00:10:45
Modem:Slave8                1080050   112       2212      00:10:25  00:10:47
Modem:Slave9                1090050   115       2224      00:10:39  00:11:05
Modem:Slave11               10B0050   107       2192      00:10:39  00:11:02
Clock:Slave12               10C000D   1         24        00:11:07  00:11:07
Dial shelf manager:Slave12  10C000E   15        2256      00:00:45  00:11:05
DSIP Test:Slave12           10C000F   0         0         never     00:11:05
```

The table below describes the significant fields shown in the display.

Table 103: show dsip ports Field Descriptions

Field	Description
Client:Portname	Client name and port name. Port Name. The port names can be determined because they are based on a uniform naming convention that includes the following elements: • Client name • Master/slave status • Slot number Any client can derive the port name of the other client it wants to talk to once it knows its physical location, using the following formula: Master/Slave Status Port Name Syntax Master *Client-Name***:Master,**for example, **Console:Master** Slave *Client-Name***:Slave***Slot*, for example, **Clock:Slave1**
Portid	Port ID. The Port ID is a 32-bit identifier comprised of **seatid** and the **port-number**. The IPC maintains a seat table which contains the seatids of all the seats in the system. A seat is where clients and ports reside. The seat ID is a function of the slot number. Port number is the sequential number of the port that is being created on a particular seat, for example: 0,1, 2, etc.
In-Msgs/	The total number of input messages that were received on a particular port.
Out-Msgs	The total number of output messages that were sent to a particular remote port.
Bytes(in/out)	The total number of bytes that were received on a particular port or sent to a remote port. The number of bytes on this port up to the time of the execution of the **show** command.
Last-i/p	Elapsed time since the last input was received on a local port.
Last-o/p	Elapsed time since the last message was sent to a particular remote port.
Last-act	Elapsed time since the connection to a remote port was opened.

Related Commands

Command	Description
show dsip clients	Lists the clients registered with DSIP on a system.
show dsip nodes	Displays information about the nodes (slots) connected by DSIP on a system.
show dsip queue	Displays the number of messages in the retransmit queue waiting for acknowledgment.
show dsip tracing	Displays DSIP tracing buffer information.
show dsip transport	Displays information about the DSIP transport statistics for the control/data and IPC packets and registered addresses.
show dsip version	Displays DSIP version information.
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

show dsip queue

To display the number of IPC messages in the transmission queue waiting for acknowledgment, use the **showdsipqueue**command in EXEC mode.

show dsip queue

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

IPC is inter-process communication. Processes communicate by exchanging messages held in queue buffers. Use the show dsip queue to display the status of these queue buffers.

Examples

The following is sample output from the **showdsipqueue**command when the system is operating correctly:

```
Router# show dsip queue

DSIP ipc queue:
---------------
There are 0 IPC messages waiting for acknowledgment in the transmit queue.
There are 0 messages currently in use by the system.
```

Related Commands

Command	Description
show dsip clients	Lists the clients registered with DSIP on a system.
show dsip nodes	Displays information about the nodes (slots) connected by DSIP on a system.
show dsip ports	Displays information about local and remote ports.
show dsip tracing	Displays DSIP tracing buffer information.
show dsip transport	Displays information about the DSIP transport statistics for the control/data and IPC packets and registered addresses.
show dsip version	Displays DSIP version information.
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

show dsip tracing

To display Distributed System Interconnect Protocol (DSIP) tracing buffer information, use the **showdsiptracing**command in EXEC mode.

show dsip tracing [{**control** | **data** | **ipc**}] [{*slot* | **entries** *entry-number* [*slot*]}]

Syntax Description

control	(Optional) Displays the control tracing buffer.
data	(Optional) Displays the data tracing buffer.
ipc	(Optional) Displays the inter-process communication tracing buffer.
slot	(Optional) Specifies a specific slot number on the dial shelf. Slot number can range from 0 to 14.
entries *entry-number*	(Optional) Specifies the number of entries to trace. Entries can be 1 to 500.

Command Modes

EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This feature allows logging of DSIP media header information. Use the **showdsiptracing**command to obtain important information of the various classes of DSIP packets (Control/Data/IPC) coming in. You must first use the **debugdsiptracing** command then use the **showdsiptracing**command to display the logged contents. To clear the information, use the **cleardsiptracing** command.

Examples

The following is sample output from the **showdsiptracing**command:

```
Router# debug dsip tracing
DSIP tracing debugging is on
Router#
Router# show dsip tracing
Dsip Control Packet Trace:
----------------------------------------------------------------------------
Dest:00e0.b093.2238 Src:0007.5387.4808 Type:200B SrcShelf:1 SrcSlot:1 MsgType:0 MsgLen:82
Timestamp: 00:00:03
----------------------------------------------------------------------------
Dest:00e0.b093.2238 Src:0007.5387.4838 Type:200B SrcShelf:1 SrcSlot:7 MsgType:0 MsgLen:82
Timestamp: 00:00:03
----------------------------------------------------------------------------
Dest:00e0.b093.2238 Src:0007.4b67.8260 Type:200B SrcShelf:1 SrcSlot:12 MsgType:0 MsgLen:82
 Timestamp: 00:00:03
----------------------------------------------------------------------------
Dest:00e0.b093.2238 Src:0007.5387.4858 Type:200B SrcShelf:1 SrcSlot:11 MsgType:0 MsgLen:82
```

```
 Timestamp: 00:00:03
----------------------------------------------------------------------------
Dest:00e0.b093.2238 Src:0007.5387.4848 Type:200B SrcShelf:1 SrcSlot:9 MsgType:0 MsgLen:82
Timestamp: 00:00:03
```

The table below describes the significant fields shown in the display.

Table 104: show dsip tracing Field Descriptions

Field	Description
Dest	The destination MAC address in the DSIP packet.
Src	The source MAC address in the DSIP packet.
Type	There are three types of DSIP packets: • Control--0x200B • IPC--0x200C • Data--0x200D
SrcShelf	The source shelf ID of the DSIP packet.
SrcSlot	The source slot of the DSIP packet.
MsgType	Used to further demultiplex Data packets. Not used for Control and IPC type packets.
MsgLen	Length of the message excluding the DSIP header.
Timestamp	Time elapsed since the packet was received.

Related Commands

Command	Description
clear dsip tracing	Clears DSIP tracing logs.
debug dsip tracing	Enables DSIP trace logging for use with the show dsip tracing commands.
show dsip clients	Lists the clients registered with DSIP on a system.
show dsip nodes	Displays information about the nodes (slots) connected by DSIP on a system.
show dsip ports	Displays information about local and remote ports.
show dsip queue	Displays the number of messages in the retransmit queue waiting for acknowledgment.
show dsip transport	Displays information about the DSIP transport statistics for the control/data and IPC packets and registered addresses.
show dsip version	Displays DSIP version information.

show dsip transport

To display information about the Distributed System Interconnect Protocol (DSIP) transport statistics for the control/data and IPC packets and registered addresses, use the **showdsiptransport**command in EXEC mode.

show dsip transport

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **showdsiptransport**command:

```
Router# show dsip transport
DSIP Transport Statistics:
 IPC : input msgs=4105, bytes=375628; output msgs=4105, bytes=248324
        total consumed ipc msgs=669;  total freed ipc msgs = 669
        transmit contexts in use = 11, free = 245, zombie = 0, invalid = 0
        ipc getmsg failures = 0, ipc timeouts=0
        core getbuffer failures=0, api getbuffer failures=0
dsip test msgs rcvd = 1200, sent = 0
 CNTL: input msgs=488, bytes=40104; output msgs=68, bytes=4080
        getbuffer failures=0
 DATA: input msgs=0, bytes=0; output msgs=426, bytes=5112

DSIP Private  Buffer Pool Hits  = 0

DSIP Registered Addresses:
 Shelf0 : Master: 00e0.b093.2238, Status=local
 Shelf1 : Slot1 : 0007.5387.4808, Status=remote
 Shelf1 : Slot5 : 0007.5387.4828, Status=remote
 Shelf1 : Slot6 : 0007.5387.4830, Status=remote
 Shelf1 : Slot7 : 0007.5387.4838, Status=remote
 Shelf1 : Slot8 : 0007.5387.4840, Status=remote
 Shelf1 : Slot9 : 0007.5387.4848, Status=remote
 Shelf1 : Slot11: 0007.5387.4858, Status=remote
 Shelf1 : Slot12: 0007.4b67.8260, Status=remote
Router#
```

The table below describes the significant fields shown in the display:

Table 105: show dsip transport Field Descriptions

Field	Description
DSIP Transport Statistics:	There are basically three kinds of communication channels between the DSIP modules running on two processors: 1. IPC: DSIP IPC-based reliable/best-effort channel. 2. CNTL: Control packet channel for DSIP modules to communicate between themselves. For example, keepalive messages and initial handshake messages between two DSIP modules are exchanged over this channel. 3. DATA: DSIP fast data packet channel.
input msgs/output msgs	The number of input/output packets on a particular channel.
bytes	The number of input bytes received or sent on a particular channel.
total consumed ipc msgs	The total number of IPC messages consumed so far from the IPC buffer pool.
total freed ipc msgs	The total number of IPC messages returned to the IPC buffer pool so far.
transmit contexts in use	DSIP for each active reliable connection to a remote port keeps a transmit context. This context holds all the important information pertaining to the remote connection, such as, destination portid, port name, number of message and bytes sent to that port etc. This is created when first time a connection is opened to a remote port and is reused for all subsequent communication to that port.
free	Free transmit context is available.
zombie	When DSIP tears down a connection to a remote slot, all the transmit contexts to that slot should return to the free pool. But instead of immediately returning to the free pool, all such contexts first end up on a zombie queue, spend their last few seconds here and then eventually return to the free queue.
invalid	Each transmit context has a magic number. While returning contexts to the free queue, if any transmit context is found to be corrupted, it is marked as invalid and is not returned to the free queue.
ipc getmsg failures	Number of times we failed to get an ipc message.
ipc timeouts	The retry timeouts of the reliable DSIP transport stack.
core getbuffer failures	The number of times DSIP transport layer has failed to allocate buffers for the IPC transport.
aip getbuffer failures	The number of times DSIP transport has failed to allocate buffers while preparing to transmit data received from the clients.
dsip test msgs received/sent	The DSIP test messages received and sent by invoking received/sent the “DSIP Test” client.

Field	Description
DSIP Private Buffer Pool Hits	DSIP by default gets all its buffers from the public buffer pools. If for some reason, it runs out of those buffers, it falls back on a DSIP private pool. This number indicates the number of times DSIP has used this fallback pool.
DSIP Registered Addresses	The MAC addresses of nodes (slots) participating in DSIP communication including the local node. The master sees N slaves whereas slave sees only master (excluding themselves). The information is presented in the following form: Shelf*X*: Master | Slot*Y* : *MACAddress* : Status= local | remote

Related Commands

Command	Description
show dsip clients	Lists the clients registered with DSIP on a system.
show dsip nodes	Displays information about the nodes (slots) connected by DSIP on a system.
show dsip ports	Displays information about local and remote DSIP ports.
show dsip queue	Displays the number of messages in the retransmit queue waiting for acknowledgment.
show dsip tracing	Displays DSIP tracing buffer information.
show dsip version	Displays DSIP version information.
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

show dsip version

To display Distributed System Interconnect Protocol (DSIP) version information, use the **showdsipversion**command in EXEC mode.

show dsip version

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **showdsipversion**command:

```
Router# show dsip version

DSIP version information:
------------------------
Local DSIP major version = 5,    minor version = 2

All feature boards are running DSIP versions compatible with router shelf

Local Clients Registered Versions:
------------------------------------
Client Name      Major Version   Minor Version
Console          52
Clock            1               1
Modem            0               0
Logger           No version      No version
Trunk            No version      No version
Async data       No version      No version
TDM              No version      No version
DSIP Test        No version      No version

Mismatched  Remote Client Versions:
-----------------------------------
```

DSIP is version-controlled software that should be identified and kept current.

Related Commands

Command	Description
show dsip clients	Lists the clients registered with DSIP on a system.
show dsip nodes	Displays information about the nodes (slots) connected by DSIP on a system.

Command	Description
show dsip ports	Displays information about local and remote DSIP ports.
show dsip queue	Displays the number of messages in the retransmit queue waiting for acknowledgment.
show dsip tracing	Displays DSIP tracing buffer information.
show dsip transport	Displays information about the DSIP transport statistics for the control/data and IPC packets and registered addresses.
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

show dtp interface

To display the desktop publishing (DTP) interface details, use the**showdtpinterface**command in user EXEC or privileged EXEC mode.

show dtp interface [*type number*]

Syntax Description

type	Interface type. For more information, use the question mark (**?**) online help function.
number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (**?**) online help function.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.4(22)T	This command was introduced in a release earlier than Cisco IOS Release 12.4(22)T.

Examples

The following is sample output from the **showdtpinterface** command:

```
Router# show dtp interface gigabitEthernet 0/0
DTP Interface Information:
  TOS/TAS/TNS:                              ACCESS/UNKNOWN/ACCESS
  TOT/TAT/TNT:                              UNKNOWN/UNKNOWN/UNKNOWN
  Neighbor address 1:                       000000000000
  Neighbor address 2:                       000000000000
  Hello timer expiration ms/state:          0/STOPPED
  Access timer expiration ms/state:         0/STOPPED
  Negotiation timer expiration ms/state:    0/STOPPED
  Multidrop timer expiration ms/state:      0/STOPPED
  FSM state:                                S1:OFF
  # times multi & trunk:                    0
  Enabled:                                  0
  In STP:                                   0
```

The following is sample output from the **showdtpinterface** command on a Catalyst 3000 series router:

```
Router# show dtp interface
DTP information for GigabitEthernet0/1:
  TOS/TAS/TNS:                                 ACCESS/AUTO/ACCESS
  TOT/TAT/TNT:                                 NATIVE/NEGOTIATE/NATIVE
  Neighbor address 1:                          000000000000
  Neighbor address 2:                          000000000000
  Hello timer expiration (sec/state):          3/RUNNING
  Access timer expiration (sec/state):         never/STOPPED
  Negotiation timer expiration (sec/state):    never/STOPPED
  Multidrop timer expiration (sec/state):      never/STOPPED
  FSM state:                                   S2:ACCESS
  # times multi & trunk                        0
  Enabled:                                     yes
  In STP:                                      no

  Statistics
```

```
----------
112868 packets received (0 good)
112868 packets dropped
    0 nonegotiate, 0 bad version, 112868 domain mismatches,
    0 bad TLVs, 0 bad TAS, 0 bad TAT, 0 bad TOT, 0 other
225650 packets output (225650 good)
    112825 native, 112825 software encap isl, 0 isl hardware native
0 output errors
0 trunk timeouts
1 link ups, last link up on Mon Mar 01 1993, 00:01:16
0 link downs
```

The table below describes the significant fields shown in the display.

Table 106: show dtp interface Field Descriptions

Field	Description
TOS	Indicates the Operational Trunk state of the port, except when the port is in the Negotiation phase. In the Negotiation phase, the status is either Trunk or Access.
TAS	Indicates the Trunk Admin state of the port, which is one of the following: ON/OFF/AUTO/DESIRABLE.
TNS	Indicates the Trunk Admin state to be sent in DTP packets when the port is in S3 or S5 DTP negotiation state.
TAT	Indicates the Trunk Admin (Encapsulation) Type of the port which is one of the following: Negotiation/Native/ISL/DOT1Q
TOT	Indicates the Trunk Operation Type or current Operational Encapsulation Type of the port, which is one of the following: Native/ISL/DOT1Q.
TNT	Indicates the Trunk Operational Type to be sent in DTP packets when the port is in either S3 or S5 DTP negotiation state.
Neighbor address 1/2	Indicates the MAC address of the neighbor connected or the Neighbor Port MAC Address 1/2 in case of multi-neighbors on the same port.
Hello timer	Indicates that a DTP advertisement is sent after the timer expires. The timer keeps running as long as DTP is enabled and the port is capable of negotiating. The time interval during negotiation is 1 second, and 30 seconds when the port is in spanning tree protocol (STP) or has reached a final DTP state.
Access timer	This timer is started when the port is in Trunk state, participates in STP (state S6), and the mode is AUTO/DESIRABLE. When the timer expires, the port is set to Access state. The interval for this timer is “10 * Hello Timer.” The interval gets reset/restarted whenever the port (which is in S6 state) receives a DTP packet and confirms its present state.
Negotiation timer	This timer is started when the port enters into an S3 or S5 DTP negotiation state. When the timer expires, the DTP state of the port moves into either Trunk/Non-Trunk. The time interval is 3 seconds and the timer is restarted if the received DTP packet changes the Trunk state or type.

Field	Description
Multidrop timer	This timer is started when the port (which is in Trunk/AUTO/DESIRABLE mode) detects multiple neighbors. The port is then configured as Access port or S4 state. When the timer expires the port moves to negotiation or S2 state. After 3 seconds, port stays in S4 state and manual intervention is needed to move it to Trunk state. The interval for this timer is "10 * Hello Timer" and it gets reset or restarted whenever the port receives a DTP packet from multiple neighbors.
FSM state	Indicates the Finite State Machine State or DTP port state. There are 5 FSM states as follows: • S1: OFF: Physical port is not in the operational state. There is no data packet transmission or receipt. • S2: ACCESS: Port state is non-Trunk and is added to the STP. • S3: NT-DTP: Port state is in negotiation phase. The port is not added to the STP and there is no data packet transmission or receipt. • S4: ACCESS-M: Port state is non-Trunk and is added to the STP. Port receives the DTP packets from multiple neighbors. • S5: T-DTP: Port is in ISL/.1Q Trunk mode. Port is not added to the STP and there is no data packet transmission or receipt. • S6: TRUNK: Port state is ISL/.1Q Trunk mode and is added to the STP. **Note** In DTP, once the final state is negotiated, the port added to the STP is either in Trunk or Access state.
# times multi & trunk	Indicates the presence of multi-neighbors and their count.
Enabled/Disabled	Indicates if DTP is enabled or disabled
In STP	Indicates if the port is added to the STP or not.

Related Commands

Command	Description
show interfaces trunk	Displays interface trunking information.

show eobc

To display the information about the Ethernet out-of-band channel (EOBC) interface, use the **showeobc** command in user EXEC or privileged EXEC mode.

show eobc

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to display the information about the EOBC interface:

```
Router>
show eobc
EOBC0/0 is up, line protocol is up
  Hardware is DEC21143, address is 0000.2100.0000 (bia 0000.2100.0000)
  MTU 0 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not set
  Unknown duplex, Unknown Speed, MII
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 25/2147483647, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     172196 packets input, 11912131 bytes
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast
     0 input packets with dribble condition detected
     172144 packets output, 11363476 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Interface EOBC0/0
Hardware is DEC21143
 dec21140_ds=0x618FB938, registers=0x3C018000, ib=0x38A9180
 rx ring entries=128, tx ring entries=256, af setup failed=0
 rxring=0x38A9280, rxr shadow=0x618FBB20, rx_head=28, rx_tail=0
 txring=0x38A9AC0, txr shadow=0x618FBD4C, tx_head=72, tx_tail=72, tx_count=0
```

```
 PHY link up
 CSR0=0xF8024882, CSR1=0xFFFFFFFF, CSR2=0xFFFFFFFF, CSR3=0x38A9280
 CSR4=0x38A9AC0, CSR5=0xF0660000, CSR6=0x320CA002, CSR7=0xF3FFA261
 CSR8=0xE0000000, CSR9=0xFFFDC3FF, CSR10=0xFFFFFFFF, CSR11=0x0
 CSR12=0xC6, CSR13=0xFFFF0000, CSR14=0xFFFFFFFF, CSR15=0x8FF80000
 DEC21143 PCI registers:
  bus_no=0, device_no=6
  CFID=0x00191011, CFCS=0x02800006, CFRV=0x02000041, CFLT=0x0000FF00
  CBIO=0x20000801, CBMA=0x48018000, CFIT=0x28140120, CFDD=0x00000400
 MII registers:
  Register 0x00:   FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF
  Register 0x08:   FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF
  Register 0x10:   FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF
  Register 0x18:   FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF
throttled=0, enabled=0, disabled=0
 rx_fifo_overflow=0, rx_no_enp=0, rx_discard=0
 tx_underrun_err=0, tx_jabber_timeout=0, tx_carrier_loss=0
 tx_no_carrier=0, tx_late_collision=0, tx_excess_coll=0
 tx_collision_cnt=0, tx_deferred=0, fatal_tx_err=0, tbl_overflow=0
 HW addr filter: 0x38D2EE0, ISL Disabled
  Entry= 0:  Addr=0000.0000.0000
  Entry= 1:  Addr=0000.0000.0000
  Entry= 2:  Addr=0000.0000.0000
  Entry= 3:  Addr=0000.0000.0000
  Entry= 4:  Addr=0000.0000.0000
  Entry= 5:  Addr=0000.0000.0000
  Entry= 6:  Addr=0000.0000.0000
  Entry= 7:  Addr=0000.0000.0000
  Entry= 8:  Addr=0000.0000.0000
  Entry= 9:  Addr=0000.0000.0000
  Entry=10:  Addr=0000.0000.0000
  Entry=11:  Addr=0000.0000.0000
  Entry=12:  Addr=0000.0000.0000
  Entry=13:  Addr=0000.0000.0000
  Entry=14:  Addr=0000.0000.0000
  Entry=15:  Addr=0000.2100.0000
Router>
```

This example shows how to display the information about the EOBC interface but excludes lines that contain the word output:

```
Router>
show eobc
| exclude output
EOBC0/0 is up, line protocol is up
  Hardware is DEC21143, address is 0000.2100.0000 (bia 0000.2100.0000)
  MTU 0 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not set
  Unknown duplex, Unknown Speed, MII
  ARP type: ARPA, ARP Timeout 04:00:00
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 25/2147483647, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
     175919 packets input, 12196443 bytes
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast
     0 input packets with dribble condition detected
     0 babbles, 0 late collision, 0 deferred
```

```
     0 lost carrier, 0 no carrier
Interface EOBC0/0
Hardware is DEC21143
 dec21140_ds=0x618FB938, registers=0x3C018000, ib=0x38A9180
 rx ring entries=128, tx ring entries=256, af setup failed=0
 rxring=0x38A9280, rxr shadow=0x618FBB20, rx_head=7, rx_tail=0
 txring=0x38A9AC0, txr shadow=0x618FBD4C, tx_head=209, tx_tail=209, tx_count=0
 PHY link up
 CSR0=0xF8024882, CSR1=0xFFFFFFFF, CSR2=0xFFFFFFFF, CSR3=0x38A9280
 CSR4=0x38A9AC0, CSR5=0xF0660000, CSR6=0x320CA002, CSR7=0xF3FFA261
 CSR8=0xE0000000, CSR9=0xFFFDC3FF, CSR10=0xFFFFFFFF, CSR11=0x0
 CSR12=0xC6, CSR13=0xFFFF0000, CSR14=0xFFFFFFFF, CSR15=0x8FF80000
 DEC21143 PCI registers:
  bus_no=0, device_no=6
  CFID=0x00191011, CFCS=0x02800006, CFRV=0x02000041, CFLT=0x0000FF00
  CBIO=0x20000801, CBMA=0x48018000, CFIT=0x28140120, CFDD=0x00000400
 MII registers:
  Register 0x00:   FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF
  Register 0x08:   FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF
  Register 0x10:   FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF
  Register 0x18:   FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF  FFFF
 throttled=0, enabled=0, disabled=0
 rx_fifo_overflow=0, rx_no_enp=0, rx_discard=0
 tx_underrun_err=0, tx_jabber_timeout=0, tx_carrier_loss=0
 tx_no_carrier=0, tx_late_collision=0, tx_excess_coll=0
 tx_collision_cnt=0, tx_deferred=0, fatal_tx_err=0, tbl_overflow=0
 HW addr filter: 0x38D2EE0, ISL Disabled
  Entry= 0:  Addr=0000.0000.0000
  Entry= 1:  Addr=0000.0000.0000
  Entry= 2:  Addr=0000.0000.0000
  Entry= 3:  Addr=0000.0000.0000
  Entry= 4:  Addr=0000.0000.0000
  Entry= 5:  Addr=0000.0000.0000
  Entry= 6:  Addr=0000.0000.0000
  Entry= 7:  Addr=0000.0000.0000
  Entry= 8:  Addr=0000.0000.0000
  Entry= 9:  Addr=0000.0000.0000
  Entry=10:  Addr=0000.0000.0000
  Entry=11:  Addr=0000.0000.0000
  Entry=12:  Addr=0000.0000.0000
  Entry=13:  Addr=0000.0000.0000
  Entry=14:  Addr=0000.0000.0000
  Entry=15:  Addr=0000.2100.0000
Router>
```

Related Commands

Command	Description
show environment alarm	Displays the information about the environmental alarm.
show environment status	Displays the information about the operational FRU status.

show errdisable detect

To display the error-disable detection status, use the **show errdisable detect** command in user EXEC or privileged EXEC mode.

show errdisable detect

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17b)SXA	This command was changed to include packet-buffer error status information.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to display the error-disable detection status:

```
Router>
show errdisable detect
ErrDisable Reason    Detection status
-----------------    ----------------
udld                 Enabled
bpduguard            Enabled
rootguard            Enabled
packet-buffer-err    Enabled
pagp-flap            Enabled
dtp-flap             Enabled
link-flap            Enabled
Router#
```

Related Commands

Command	Description
errdisable detect cause	Enables the error-disable detection.

show errdisable recovery

To display the information about the error-disable recovery timer, use the **show errdisable recovery** command in EXEC mode.

show errdisable recovery

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to display the information about the error-disable recovery timer:

```
Router#
show errdisable recovery
ErrDisable Reason    Timer Status
-----------------    --------------
udld                 Enabled
bpduguard            Enabled
rootguard            Enabled
pagp-flap            Enabled
dtp-flap             Enabled
link-flap            Enabled
Timer interval:300 seconds
Interfaces that will be enabled at the next timeout:
Interface    Errdisable reason    Time left(sec)
---------    -----------------    --------------
Fa9/4           link-flap             279
```

Related Commands

Command	Description
errdisable recovery	Configures the recovery mechanism variables.
show interfaces status	Displays the interface status or a list of interfaces in an error-disabled state on LAN ports only.

show esmc

To display the Ethernet synchronization message channel (ESMC) processes on a device, use the **show esmc** command in privileged EXEC mode.

show esmc [{**detail** | **interface** *type number*}]

Syntax Description

detail	(Optional) Provides a detailed display of ESMC processes.
interface *type number*	(Optional) Specifies the interface type and interface number. For more information, use the question mark (?) online help function.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)S	This command was introduced.
15.1(2) SNI	This command was introduced into Cisco ASR 901 Aggregation Services Router.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Examples

The following example shows the ESMC processes enabled on a device:

```
Device# show esmc detail

Interface: GigabitEthernet0/0/0
Administrative configurations:
  Mode: Synchronous
  ESMC TX: Enable
  ESMC RX : Enable
  QL RX configured : NA
  QL TX configured : NA
Operational status:
  Port status: UP
  QL Receive: QL-SSU-B
  ESMC Information rate : 1 packet/second
  ESMC Expiry: 5 second
```

The table below describes the significant fields shown in the display.

Table 107: show esmc Field Descriptions

Field	Description
Mode	Synchronous or asynchronous mode of packet transmission.
ESMC TX	Option for transmitting ESMC data.
ESMC RX	Option for receiving ESMC data.

Field	Description
QL RX configured	Quality level receive configuration.
QL TX configured	Quality level transmit configuration.
ESMC Information rate	Rate at which ESMC information Protocol Data Unit (PDU) is transmitted in packet per second.
ESMC Expiry	Duration in which the ESMC receipt is expired.

Related Commands

Command	Description
esmc mode ql-disabled	Disables the ESMC on an interface.
esmc process	Enables the ESMC process in a device.
show interfaces accounting	Displays the number of packets of each protocol type that have been sent through all configured interfaces.

show etherchannel

To display EtherChannel information for a channel, use the **showetherchannel** command in privileged EXEC mode.

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers
show etherchannel [*channel-group*] {**port-channel** | **brief** | **detail** | **summary** | **port** | **load-balance**}

Cisco Catalyst Switches
show etherchannel [*channel-group*] {**port-channel** | **brief** | **detail** | **summary** | **port** | **load-balance** | **protocol**} [*expression*]

Syntax Description

channel -group	(Optional) Number of the channel group. If you do not specify a value for the *channel -group* argument, all channel groups are displayed.
port -channel	Displays port channel information.
brief	Displays a summary of EtherChannel information.
detail	Displays detailed EtherChannel information.
summary	Displays a one-line summary per channel group.
port	Displays EtherChannel port information.
load -balance	Displays load-balance information.
protocol	Displays the enabled protocol.
expression	(Optional) Expression in the output to use as a reference point.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(7)XE	This command was introduced on Cisco Catalyst 6000 family switches.
12.1(3a)E3	This command was modified. The number of valid values for the *channel -group* argument were changed.
12.1(5c)EX	This command was modified. The number of valid values for the *channel-group* argument were changed.
12.2(2)XT	This command was modified to support switchport creation on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(14)SX	This command was implemented on the Supervisor Engine 720.
12.2(17a)SX1	This command was modified. The output of the **showetherchannelload-balance** command was changed to include IPv6 information. The display was changed to include Multiprotocol Label Switching (MPLS) information.

Release	Modification
12.2(17d)SXB	This command was modified to support the Supervisor Engine 2.
12.2(8)T	This command was modified to support switchport creation.
12.2(33)SXH	This command was modified. The output of the **showetherchannelport-channel** and the **showetherchanneldetail**commands was changed to include Link Aggregation Control Protocol (LACP) fast switchover status. The number of valid values for the *channel -group* argument was changed.
12.2(33)SRC	This command was modified. The output of the **showetherchannelport-channel** and the **showetherchanneldetail**commands was changed to show the status of the LACP Single Fault Direct Load Balance Swap feature, to show the last applied hash distribution algorithm, and to include LACP fast switchover status.
12.2(33)SXI3	This command was modified. The output of the **showetherchannelsummary**, **showetherchannelport-channel**, and **showetherchanneldetail** commands was changed to show the standalone disable option.

Usage Guidelines

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

The *channel-group* argument supports six EtherChannels and eight ports in each channel.

If you do not specify a value for the *channel-group* argument, all channel groups are displayed.

Cisco Catalyst Switches

The number of valid values for the *channel-group* argument depends on the software release. For software releases prior to Cisco IOS Release 12.1(3a)E3, valid values are from 1 to 256; for Cisco IOS Release 12.1(3a)E3, 12.1(3a)E4, and 12.1(4)E1, valid values are from 1 to 64. Cisco IOS Release 12.1(5c)EX and later support a maximum of 64 values ranging from 1 to 256. Cisco IOS Release 12.2(33)SXH supports a maximum of 64 values ranging fro m 1 to 282.

If you do not specify a value for the *channel-group* argument, all channel groups are displayed.

In the output, the Passive port list field is displayed for Layer 3 port channels only. This field means that the physical interface, which is still not up, is configured to be in the channel group (and indirectly in the only port channel in the channel group).

The *channel-group*values from 257 to 282 are supported on the Catalyst 6500 series Cisco Services Module (CSM) and the Catalyst 6500 series Firewall Services Module (FWSM) only.

In the output, the Passive port list field is displayed for Layer 3 port channels only. This field means that the physical interface, which is still not up, is configured to be in the channel group (and indirectly is the only port channel in the channel group).

If the interface is configured as part of the channel in ON mode, the**showetherchannelprotocol** command displays Protocol: - (Mode ON).

In the output of the **showetherchannelsummary** command, the following conventions apply:

- In the column that displays the protocol that is used for the channel, if the channel mode is ON, a hyphen (-) is displayed.
- For LACP, multiple aggregators are supported. For example, if two different bundles are created, Po1 indicates the primary aggregator, and Po1A and Po1B indicates the secondary aggregators.

In the output of the **showetherchannelload-balance** command, the following conventions apply:

- For EtherChannel load balancing of IPv6 traffic, if the traffic is bridged onto an EtherChannel (for example, it is a Layer 2 channel and traffic in the same VLAN is bridged across it), the traffic is always load balanced by the IPv6 addresses or src, dest, or src-dest, depending on the configuration. For this reason, the switch ignores the MAC/IP/ports for bridged IPv6 traffic. If you configure src-dst-mac, the src-dst-ip(v6) address is displayed. If you configure src-mac, the src-ip(v6) address is displayed.
- IPv6 traffic that is routed over a Layer 2 or a Layer 3 channel is load balanced based on MAC addresses or IPv6 addresses, depending on the configuration. The MAC/IP and the src/dst/src-dst are supported, but load balancing that is based on Layer 4 ports is not supported. If you use the **port** keyword, the IPv6 addresses or either src, dst, or src-dst, is displayed.

Examples

Protocol Information

The following example shows how to display the enabled protocol:

```
Router# show etherchannel protocol
Channel-group listing:
                ----------------------- 
Group: 12
----------
Protocol:  PAgP
Group: 24
----------
Protocol:   -  (Mode ON)
Router#
```

Port Channel Information for a Specific Group

The following example shows how to display port channel information for a specific group:

```
Router# show etherchannel 12 port-channel
Group: 12
----------
                Port-channels in the group:
                ----------------------
Port-channel: Po1
------------
Age of the Port-channel   = 143h:01m:12s
Logical slot/port   = 14/1           Number of ports = 2
GC                  = -              HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            = LACP
Fast-switchover     = enabled
Ports in the Port-channel:
Index   Load   Port    EC state
------+------+------+------------
  0     55     Fa4/1   active
  1     AA     Fa4/2   active
Time since last port bundled:    16h:28m:58s    Fa4/1
Time since last port Un-bundled: 16h:29m:00s    Fa4/4
```

The following example shows that direct load swapping is enabled.

```
Router# show etherchannel 15 port-channel
                Port-channels in the group:
Port-channel: Po15    (Primary Aggregator)
Age of the Port-channel   = 0d:18h:16m:49s
Logical slot/port   = 14/7          Number of ports = 1
HotStandBy port = null
Port state              = Port-channel Ag-Inuse
Protocol                =   LACP
! The following line of output is added with support
of the LACP Single Fault Direct Load Swapping feature. !
Direct Load Swap = enabled
Ports in the Port-channel:
Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     FF     Fa4/1    Active    8
Time since last port bundled:    0d:00h:06m:12s    Fa4/1
```

Load Balancing

The following examples show how to display load-balancing information:

```
Router#
 show etherchannel load-balance
Source XOR Destination mac address
Router#
 show etherchannel load-balance
EtherChannel Load-Balancing Configuration:
        dst-mac
        mpls label-ip
EtherChannel Load-Balancing Addresses Used Per-Protocol:
Non-IP: Destination MAC address
  IPv4: Destination MAC address
  IPv6: Destination MAC address (routed packets)
        Destination IP address (bridged packets)
  MPLS: Label or IP
```

Summary Information for a Specific Group

The following example shows how to display a summary of information for a specific group:

```
Router#
show etherchannel 1 brief
Group state = L3
Ports: 2   Maxports = 8
port-channels: 1 Max port-channels = 1
Partner's information:
```

The following example shows the hash distribution algorithm that was last applied:

```
Router# show etherchannel
 10 summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator
```

```
<snip>
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
10     Po10(RU)         LACP      Gi3/7(P)       Gi3/9(P)
! The following line of output is added with support
of the EtherChannel Load Distribution feature. !
Last applied Hash Distribution Algorithm: Fixed
Router#
```

Detailed Information for a Specific Group

The following example shows how to display detailed information for a specific group:

```
Router#
show etherchannel 12 detail
Group state = L2
Ports: 1   Maxports = 8
Port-channels: 1 Max Port-channels = 1
Protocol:   PAgP
Fast-switchover = enabled
                Ports in the group:
                -------------------
Port: Fa5/2
------------
Port state    = Down Not-in-Bndl
Channel group = 12          Mode = Desirable-Sl     Gcchange = 0
Port-channel  = null        GC   = 0x00000000          Pseudo port-channel = Po1
2
Port index    = 0           Load = 0x00        Protocol =   PAgP
Flags:  S - Device is sending Slow LACPDUs F - Device is sending fast LACPDUs
        A - Device is in active mode       P - Device is in passive mode
Local information:
                            LACP Port    Admin     Oper    Port     Port
Port      Flags   State     Priority      Key      Key     Number   State
Fa4/1     SA      bndl      32768         100      100     0xc1     0x75
Partner's information:
         Partner                Partner               Partner
Port     System ID              Port Number    Age    Flags
Fa4/1    8000,00b0.c23e.d861    0x81            14s    SP
         LACP Partner    Partner     Partner
         Port Priority   Oper Key    Port State
         32768            128         0x81
Age of the port in the current state: 16h:27m:42s
                Port-channels in the group:
                ----------------------
Port-channel: Po12
------------
Age of the Port-channel   = 04d:02h:52m:26s
Logical slot/port   = 14/1          Number of ports = 0
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel Ag-Not-Inuse
Protocol            =   PAgP
```

Note When LACP 1:1 redundancy is configured, the **showetherchanneldetail** command also displays fast-switchover status information.

One-Line Summary per Channel Group

The following example shows how to display a one-line summary per channel group:

```
Router#
show etherchannel summary
U-in use  I-in port-channel   S-suspended   D-down  i-stand-alone  d-default
Group Port-channel  Ports
----- ------------  ---------------------------------------------------------
1     Po1(U)        Fa5/4(I)  Fa5/5(I)
2     Po2(U)        Fa5/6(I)  Fa5/7(I)
255                 Fa5/9(i)
256                 Fa5/8(i)
```

Port Information for All Groups

The following example shows how to display EtherChannel port information for all ports and all groups:

```
Router#
show etherchannel port
                Channel-group listing:
                -----------------------
Group: 1
----------
                Ports in the group:
                -------------------
Port: Fa5/4
------------
Port state    = EC-Enbld Down Not-in-Bndl Usr-Config
Channel group = 1           Mode = Desirable     Gcchange = 0
Port-channel  = null        GC   = 0x00000000    Psudo-agport = Po1
Port indx     = 0           Load = 0x00
Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.        P - Device learns on physical port.
Timers: H - Hello timer is running.        Q - Quit timer is running.
        S - Switching timer is running.    I - Interface timer is running.
Local information:
                                Hello    Partner  PAgP     Learning  Group
Port      Flags State   Timers  Interval Count   Priority   Method  Ifindex
Fa5/4     d     U1/S1           1s       0        128        Any      0

Age of the port in the current state: 02h:40m:35s
Port: Fa5/5
------------
Port state    = EC-Enbld Down Not-in-Bndl Usr-Config
Channel group = 1           Mode = Desirable     Gcchange = 0
Port-channel  = null        GC   = 0x00000000    Psudo-agport = Po1
Port indx     = 0           Load = 0x00
Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.        P - Device learns on physical port.
Timers: H - Hello timer is running.        Q - Quit timer is running.
        S - Switching timer is running.    I - Interface timer is running.
```

Port Information for a Specific Group

The following example shows how to display the information about the EtherChannel port for a specific group:

```
Router#
show etherchannel 1 port
                Channel-group listing:
                -----------------------
Group: 1
----------
                Ports in the group:
                -------------------
Port: Fa5/4
------------
Port state    = EC-Enbld Down Not-in-Bndl Usr-Config
Channel group = 1           Mode = Desirable     Gcchange = 0
Port-channel  = null        GC   = 0x00000000    Psudo-agport = Po1
Port index    = 0           Load = 0x00        Protocol =   LACP
Flags:  S - Device is sending Slow LACPDUs F - Device is sending fast LACPDUs
        A - Device is in active mode       P - Device is in passive mode
Local information:
                            LACP Port    Admin     Oper    Port     Port
Port      Flags   State     Priority      Key      Key     Number   State
Fa5/4     SA      bndl      32768         100      100     0xc1     0x75
Partner's information:
         Partner                Partner               Partner
Port     System ID              Port Number    Age    Flags
Fa5/4    8000,00b0.c23e.d861    0x81            14s    SP
         LACP Partner    Partner     Partner
         Port Priority   Oper Key    Port State
         32768            128         0x81
Age of the port in the current state: 04d:02h:57m:38s
```

Port Channel Information for the Standalone Disabled Option

The following example shows the **showetherchannelsummary** command output with a port in suspended state:

```
Router# show etherchannel 42 summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
Number of channel-groups in use: 8
Number of aggregators:           8
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
2      Po42(SU)        LACP      Fa1/17(s)  Fa1/18(P)  Fa1/19(P)  Fa1/20(P)
```

The following example shows the **showetherchannelport-channel** command output with the status of Standalone Disable option:

```
Router# show etherchannel 42 port-channel
```

```
                Port-channels in the group:
                ----------------------
Port-channel: Po42    (Primary Aggregator)
------------
Age of the Port-channel   = 0d:21h:28m:22s
Logical slot/port   = 14/42          Number of ports = 3
HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   LACP
Fast-switchover     = disabled
Load share deferral = disabled
Standalone Disable  = enabled
Ports in the Port-channel:
Index   Load      Port          EC state       No of bits
------+------+------------+------------------+-----------
 2      49         Fa1/18             Active   3
 1      92         Fa1/19             Active   3
 3      24         Fa1/20             Active   2
Time since last port bundled:    0d:03h:37m:07s    Fa1/18
Time since last port Un-bundled: 0d:03h:34m:27s    Fa1/17
Last applied Hash Distribution Algorithm: Fixed
```

The following example shows the **showetherchanneldetail** command output with the status of Standalone Disable option:

```
Router# show etherchannel 42 detail

Group state = L2
Ports: 4   Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol:   LACP
Minimum Links: 2
Standalone Disable: enabled
                Ports in the group:
                -------------------
Port: Fa1/17
------------
Port state    = Up Cnt-bndl Suspend Not-in-Bndl
Channel group = 42           Mode = Active      Gcchange = -
Port-channel  = null        GC   =   -         Pseudo port-channel = Po2
Port index    = 0           Load = 0x00        Protocol =   LACP
Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.
Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
Fa1/17    FP      susp      1             0x2       0x2     0x112       0x82
Partner's information:
          Partner Partner   LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State     Port Priority Admin Key Oper Key Port Number Port State
Fa1/17    FP      susp      1             0x0       0x2      0x312       0x36
Age of the port in the current state: 0d:03h:44m:04s
Port: Fa1/18
------------
Port state    = Up Mstr In-Bndl
Channel group = 42           Mode = Active      Gcchange = -
Port-channel  = Po2         GC   =   -         Pseudo port-channel = Po2
Port index    = 2           Load = 0x49        Protocol =   LACP
Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.
Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
```

```
Fa1/18    SA      bndl      2             0x2       0x2     0x113       0x3D
Partner's information:
          Partner Partner   LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State     Port Priority Admin Key Oper Key Port Number Port State
Fa1/18    SA      bndl      2             0x0       0x2      0x313       0x3D
Age of the port in the current state: 0d:03h:43m:24s
Port-channels in the group:
Port-channel: Po42    (Primary Aggregator)
Age of the Port-channel   = 0d:21h:34m:45s
Logical slot/port   = 14/42          Number of ports = 3
HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   LACP
Fast-switchover     = disabled
Load share deferral = disabled
Standalone Disable  = enabled
Ports in the Port-channel:
Index   Load      Port          EC state       No of bits
------+------+------------+------------------+-----------
 2      49         Fa1/18            Active   3
 1      92         Fa1/19            Active   3
 3      24         Fa1/20            Active   2
Time since last port bundled:    0d:03h:43m:30s    Fa1/18
Time since last port Un-bundled: 0d:03h:40m:50s    Fa1/17
Last applied Hash Distribution Algorithm: Fixed
```

Related Commands

Command	Description
channel-group	Assigns and configures an EtherChannel interface to an EtherChannel group.
channel-protocol	Sets the protocol that is used on an interface to manage channeling.
interface port-channel	Accesses or creates the IDB port channel.

show etherchannel load-balancing

To display the load-balancing method applied to Gigabit EtherChannel (GEC) interfaces, use the **showetherchannelload-balancing** command in user EXEC or privileged EXEC mode.

show etherchannel load-balancing

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. Information about the port-channel configuration and flow-based load balancing was added to the output.

Usage Guidelines

The **showetherchannelload-balancing** command shows which load-balancing method is applied to the port channels of a GEC interface, both at the global level and for each port channel.

There are two methods of load balancing on a GEC interface:

- VLAN-manual--All packets forwarded over the same VLAN subinterface are considered part of the same flow and are mapped to the member link specified in the configuration.
- Flow-based--Traffic flows are mapped to different member links based on the packet header.

Examples

The following example shows output from this command for a port channel configured with VLAN-manual load balancing:

```
Router# show etherchannel load-balancing

EtherChannel Load-Balancing Method:
Global LB Method: vlan-manual

  Port-Channel:                       LB Method
    Port-channel1                   :  vlan-manual
```

The table below describes the significant fields shown in the display.

Table 108: show etherchannel load-balancing Field Descriptions

Field	Description
Global LB Method	Load balancing method set globally for all port channels with the **port-channelload-balancingvlan-manual** command.
Port Channel LB Method	Load balancing method set for the specific port channels with the **load-balancing**command. This configuration takes precedence over the global configuration.

Related Commands

Command	Description
load-balancing	Applies a load-balancing method to a GEC interface.
port-channel load-balancing vlan-manual	Applies the VLAN-manual load-balancing method globally to all GEC interfaces.
show interfaces port-channel etherchannel	Displays the load-balancing bucket distribution currently in use for a GEC interface.

show fabric

To display the information about the crossbar fabric, use the **showfabric** command in EXEC mode.

show fabric [**active**]
show fabric {**channel-counters** | **errors** | **status**} [{*slot* | **all**}]
show fabric switching-mode [**module** {*slot* | **all**}]
show fabric utilization [{*slot* | **all**}]

Syntax Description

active	(Optional) Displays the redundancy status for the Switch Fabric Module.
channel-counters	Displays the fabric channel-counter information.
errors	Displays the errors that are associated with the crossbar fabric; see the "Usage Guidelines" section for additional information.
status	Displays the current status of the fabric channel.
slot	(Optional) Number of the slot.
all	(Optional) Displays the information for all modules using the crossbar fabric.
switching-mode	Displays the module switching mode; see the "Usage Guidelines" section for additional information.
module *slot*	(Optional) Displays the switching mode for the specified slot.
module all	(Optional) Displays the switching mode for all installed modules.
utilization	Displays the percentage utilization for each fabric channel.

Command Default

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 32.

If you specify *slot*, the information is displayed for the specified slot. If you specify **all**, the information for all slots using the crossbar fabric is displayed. If you do not specify *slot* or **all**, the display is the same as if you entered **all**.

To display all the related crossbar fabric information, enter the **showfabric** command without keywords.

A fabric channel is each connection between a module and the crossbar fabric module. Each module can have zero, one, or two fabric channels. The more fabric channels that a module has, the more overall bandwidth is available to the module.

The following errors are associated with the crossbar fabrics:

- Synchronization errors--General errors are the most common types of errors.
- Heartbeat errors--The supervisor engine sends out periodic heartbeat packets to each module using the crossbar fabric. If any of these modules or the crossbar fabric fail to detect heartbeat packets for a period of time, this error is reported.
- CRC errors--All packets crossing the crossbar fabric are CRC protected. If any of the ASICs between a module and the crossbar fabric module detect a CRC error, this error is reported.

The three types of fabric switching modes are as follows:

- Bus--Packets that travel across the traditional backplane and that are shared by all modules to be switched by the supervisor engine. Modules without the crossbar fabric connectors are restricted to this mode. The 48-port 10/100TX RJ-45 module is an example of this module type.
- Crossbar--Packets with headers only that travel across the traditional backplane to be switched by the supervisor engine and that travel across the crossbar fabric. The 16-port Gigabit Ethernet GBIC switching module is an example of this module type.
- dCEF--Packets that are switched by the module and that travel across the crossbar fabric. The 16-port Gigabit Ethernet GBIC switching module and the 16-port Gigabit Ethernet module are examples of this module type. The 16-port Gigabit Ethernet GBIC switching module can be in any of these three modes, but the 16-port Gigabit Ethernet module can only be in dCEF mode.

The threshold information is shown only when you enter the **nofabricswitching-modeallowtruncated** command.

In the **showfabricswitching-mode** command output, the possible global switching modes are as follows:

- Flow-through (Bus)--Mode that the switch uses for traffic between nonfabric-enabled modules and for traffic between a nonfabric-enabled module and a fabric-enabled module. In this mode, all traffic passes between the local bus and the supervisor engine bus.
- Truncated--Mode that the switch uses for traffic between fabric-enabled modules when both fabric-enabled and nonfabric-enabled modules are installed. In this mode, the switch sends a truncated version of the traffic (the first 64 bytes of the frame) over the switch fabric channel.
- Compact--Mode that the switch uses for all traffic when only fabric-enabled modules are installed. In this mode, a compact version of the DBus header is forwarded over the switch fabric channel, which provides the best possible performance.

In the **showfabricswitching-mode** command output , depending on the supervisor engine installed, the following messages appear:

- With a Supervisor Engine 2, this message is included in the output:

```
An enabled Switch Fabric is not required for the system to operate
```

- With a Supervisor Engine 720, this message is included in the output:

```
Fabric module is not required for system to operate
```

Examples

This example shows how to display the redundancy status of the Switch Fabric Module:

```
Router# show fabric active
Active fabric card in slot 5
No backup fabric card in the system
Router#
```

This example shows how to display the channel-counter information:

```
Router# show fabric channel-counters
slot channel   rxErrors   txErrors  txDropped
    1       0          0          0          0
Router#
```

This example shows how to display the errors that are associated with the crossbar fabric:

```
Router# show fabric errors
Module errors:
slot     channel        crc      hbeat       sync      DDR sync
   1           0          0          0          0             0
   8           0          0          0          0             0
   8           0          0          0          0             0
   9           0          0          0          0             0
Fabric errors:
slot     channel       sync     buffer    timeout
   1           0          0          0          0
   8           0          0          0          0
   8           0          0          0          0
   9           0          0          0          0
Router#
```

This example shows how to display the module switching mode:

```
Router# show fabric switching-mode
Global switching mode is Truncated
An enabled Switch Fabric is not required for the system to operate
Modules are allowed to operate in bus mode
Truncated mode is not allowed unless threshold is met
Threshold for truncated mode operation is 2 SFM-capable cards
 Module Slot     Switching Mode
     1           Bus
     2           Crossbar
     3           Crossbar
     4           Bus
     5           No Interfaces
     7           DCEF
     9           DCEF
Router#
```

This example shows how to display the fabric-channel status:

```
Router# show fabric status
slot    channel      speed           module           fabric
                                      status            status
    1          0         8G              OK                OK
    5          0         8G              OK      Up- Timeout
    6          0        20G              OK     Up- BufError
```

```
    8          0          8G              OK               OK
    8          1          8G              OK               OK
    9          0          8G    Down- DDRsync              OK
Router#
```

This example shows how to display the percentage utilizations for all fabric-enabled channels:

```
Router# show fabric utilization all
slot    channel  Ingress %   Egress %
    1          0          0          0
crc       hbeat       sync       sync
    1          0          0          0          0          0
Router#
```

show fm features

To display the information about the feature manager, use the **showfmfeatures** command in user EXEC or privileged EXEC mode.

show fm features

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to display the information about the feature manager:

```
Router>
show fm features
Designated MSFC:1 Non-designated MSFC:1
Redundancy Status:designated
Interface:FastEthernet2/10 IP is enabled
  hw[EGRESS] = 1, hw[INGRESS] = 1
  hw_force_default[EGRESS] = 0, hw_force_default[INGRESS] = 0
  mcast = 0
  priority = 2
  reflexive = 0
  inbound label:1
        protocol:ip
          feature #:1
          feature id:FM_IP_ACCESS
          ACL:106
  outbound label:2
        protocol:ip
          feature #:1
          feature id:FM_IP_ACCESS
          ACL:106
Interface:FastEthernet2/26 IP is enabled
  hw[EGRESS] = 1, hw[INGRESS] = 0
  hw_force_default[EGRESS] = 0, hw_force_default[INGRESS] = 1
  mcast = 0
  priority = 2
  reflexive = 0
  inbound label:24
        protocol:ip
          feature #:1
          feature id:FM_IP_ACCESS
          ACL:113
  outbound label:3
```

```
        protocol:ip
          feature #:1                                           feature
id:FM_IP_WCCP
          Service ID:0
          Service Type:0
Interface:Vlan55 IP is enabled
  hw[EGRESS] = 1, hw[INGRESS] = 1
  hw_force_default[EGRESS] = 0, hw_force_default[INGRESS] = 0
  mcast = 0
  priority = 2
  reflexive = 0
  inbound label:4
        protocol:ip
          feature #:1
          feature id:FM_IP_ACCESS
          ACL:111
Interface:Vlan101 IP is enabled
  hw[EGRESS] = 1, hw[INGRESS] = 1
  hw_force_default[EGRESS] = 0, hw_force_default[INGRESS] = 0
  mcast = 0
  priority = 2
  reflexive = 0
  inbound label:5
        protocol:ip
          feature #:1
          feature id:FM_IP_ACCESS
          ACL:101
  outbound label:6
        protocol:ip
          feature #:1
          feature id:FM_IP_ACCESS
          ACL:101
Router>
```

This example shows how to display the lines of feature manager information starting with the line that begins with Redundancy:

```
Router>
show fm features | begin Redundancy
Redundancy Status: designated
Router>
```

Related Commands

Command	Description
show fm summary	Displays a summary of FM Information.

show fm inband-counters

To display the number of inband packets that are sent by the Multilayer Switching Feature Card (MSFC) for server load balancing (SLB) and Web Cache Coprocessor Protocol (WCCP), use the **showfminband-counters** command in privileged EXEC mode.

show fm inband-counters

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The output display for the **showfminband-counters** command includes the number of SLB inband packets that are sent by the MSFC and the number of WCCP inband packets that are sent by the MSFC.

If CBAC is configured, the command output displays the number of packets that are sent for CBAC by the MSFC.

Examples

This example shows how to display the number of SLB and WCCP inband packets that are sent by the MSFC:

```
Router# show fm inband-counters
Inband Packets Sent
 Slot  WCCP          SLB
 1     0             0
 2     0             0
 3     0             0
 4     0             0
 5     0             0
 6     0             0
 7     0             0
 8     0             0
 9     0             0
 10    0             0
 11    0             0
 12    0             0
 13    0             0
Router#
```

show gnss

To display the output of the GNSS configuration, use the **show gnss** command in privileged EXEC mode.

show gnss [{**location** | **satellite** | **status** | **time** | **device**}]

Syntax Description

location	(Optional) Displays the location of the GNSS module.
satellite	(Optional) Displays the satellites configured or detected by the GNSS module.
status	(Optional) Displays the status of the GNSS module.
time	(Optional) Displays the time on the GNSS module.
device	(Optional) Displays the hardware information of the active GNSS module.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.17	This command was introduced.

Usage Guidelines

Use this command to verify the GNSS configuration.

Examples

The following examples show the output generated by this command:

```
Router# show gnss

Current GNSS Location:

LOC: 12:56.183600 N 77:41.768000 E 819.10 m

Router# show gnss satellite all

All Satellites Info:

SV PRN No   Channel No       Acq Flg    Ephemeris Flg     SV Type     Sig Strength
----------------------------------------------------------------------------------
21          0                1          1                 0           47
14          1                1          1                 0           48
18          2                1          1                 0           49
22          3                1          1                 0           46
27          4                1          1                 0           44
24          5                1          1                 0           44
31          6                1          1                 0           47

Router# show gnss status

GNSS status:

GNSS device: detected
Lock status: Power-up
Receiver Status: Auto
Clock Progress: Phase Locking
```

```
Survey progress: 100
Satellite count: 7
Holdover Duration: 0
PDOP: 1.01 TDOP: 1.00
HDOP: 0.71 VDOP: 0.72
Minor Alarm: ANTENNA_OPEN NOT_DISCIPLINING_OSC
Major Alarm: None

Router# show gnss time

Current GNSS Time:

Time: 2015/11/30 10:20:33 UTC Offset: 17

Router# show gnss device
GNSS device:

  Serial number: FOC2130ND5X
  Firmware version: 1.4
  Firmware update progress: NA
  Authentication: Passed
```

In the **show gnss device** command output, serial number and authentication information is shown only for pluggable GNSS module like Cisco ASR 903. It is not shown for Cisco ASR 920.

show gtp

To display information related to Enhanced Wireless Access Gateway (EWAG) General Packet Radio Service (GPRS) Tunneling Protocol (GTP), use the **show gtp** command in privileged EXEC mode.

show gtp {**apn** [**statistics**] {*apn-index* | **all**} | **mcsa statistics** | **parameters** | **path** {**all** | [{**statistics**}] **remote-address** *path-address* [{**vrf** *vrf-name*}]} | **pdp-context** {**all** | **apn** *apn-index* | **imsi** *imsi-value* [{**detail**}] | **ms-address** *end-user-address* [{**vrf** *vrf-name*}] [{**detail**}] | **msisdn** *msisdn-value* [{**detail**}] | **teid-u** *user-teid* [{**detail**}]} | **statistics** | **tunnel** *interface type*}

Syntax Description

apn	Displays Access Point Name (APN) information.
apn-index	Index of the APN.
all	Displays information about all APNs.
statistics	(Optional) Displays information about APN counters.
mcsa statistics	Displays statistical information about Mobile Client Service Abstraction (MCSA) counters.
parameters	Displays information about GTP parameters.
path	Displays information about GTP path.
all	Displays information about all GTP paths.
statistics	Displays statistics related to a path.
remote-address *path-address*	Displays GTP path for a specified path address.
vrf *vrf-name*	Specifies the virtual routing and forwarding (VRF) containing the IP address.
pdp-context	Displays information about GTP Packet Data Protocol (PDP) data structures.
all	Displays information about all PDPs.
apn *apn_index*	Displays information about PDPs for the specified APN.

imsi *imsi_value*	Displays information about PDPs for the specified International Mobile Subscriber Identity (IMSI) value.
detail	Displays information about PDPs for the specified IMSI value in detail.
ms-address *end-user-address*	Displays information about PDPs for a specified end-user IPv4 address.
teid-u *user-teid*	Displays information about PDPs for a specified Tunnel Endpoint Identifier (TEID) user.
statistics	Displays information about GTP counters.
tunnel *interface type*	Displays information about GTP tunnels.

Command Default

This command has no defaults.

Command Modes

Previliged EXEC (#)

Command History

Release	Modification
Cisco IOS Release XE 3.8S	This command was introduced.

Usage Guidelines

Examples

The following is sample output of **show gtp apn** command:

```
Device# show gtp apn 1

apn_index   : 1            apn_name = starent.com
GGSN Addr   : 10.1.2.1
Primary DNS : 10.1.2.1
DHCP Addr   : 10.10.197.1     DHCP Lease: 6000
Tunnel MTU  : 1500
Number of active PDPs in this APN : 0

Default GW      Prefix Length Name              MAC Address     PDP Count
```

The table below describes the significant fields shown in the display.

Table 109: show gtp apn Field Descriptions

Field	Description
apn_index	Index of the APN.
apn_name	Name of the APN.
GGSN Addr	Gateway GPRS Support Node (GGSN) IP address of the APN.
Primary DNS	Primary Domain Name System (DNS) Address of the APN.
DHCP Addr	DHCP Address of the APN
Tunnel MTU	Maximum Transmission unit of a tunnel.
DHCP Lease	DHCP lease time in seconds.
Number of active PDPs in this APN	Number of active PDPs in the APN.

Related Commands

Command	Description
debug gtp	Debugs EWAG GTP.
gtp	Enables EWAG GTP.

show hspw-aps-icrm

To view information about hot standby pseudowires (HSPW), use the **showhspw-aps-icrm** command in privileged EXEC mode.

show hspw-aps-icrm {**group** *group-id* | **all**}

Syntax Description

group	Specifies the HSPW Automatic Protection Switching (APS) group.
group-id	HSPW APS group identifier.
all	Displays all the HSPW APS and inter chassis redundancy manager (ICRM) groups.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS 15.2(1)S	This command was introduced.
Cisco IOS XE 3.11S	This command was integrated into Cisco IOS XE Release 3.11S.

Usage Guidelines

Use this command to display information about a particular HSPW APS group or all HSPW APS and ICRM groups.

The following is sample output from the **show hspw-aps-icrm** command when **group** *group-id* is used to display information about a particular HSPW APS group:

```
Router# show hspw-aps-icrm group 100

ICRM group id 100, Flags : My core isolated No,Peer core isolated No,
State Connect
APS Group id 1 hw_if_index 33 APS valid:Yes
Total aps grp attached to ICRM group 100 is 1
```

Displaying Information About All HSPW APS and ICRM Groups

The following is sample output from the **show hspw-aps-icrm** command when **all** is used to display information about all the HSPW APS and ICRM groups:

```
Router# show hspw-aps-icrm all

ICRM group id 100, Flags : My core isolated No,Peer core isolated No,
State Connect
APS Group id 1 hw_if_index 33 APS valid:Yes
Total aps grp attached to ICRM group 100 is 1 ICRM group count
attached to MR-APS HSPW feature is 1
```

Related Commands

Command	Description
show aps	Displays information about the current APS feature on the router.

show hub

To display information about the hub (repeater) on an Ethernet interface of a Cisco 2505 or Cisco 2507 router, use the **showhub** command in user EXEC or privileged EXEC mode.

show hub commandshow hub [**ethernet** *number* [*port* [*end-port*]]]

Syntax Description

ethernet	(Optional) Indicates that this is an Ethernet hub.
number	(Optional) Hub number, starting with 0. Because there is currently only one hub, this number is 0.
port	(Optional) Port number on the hub. On the Cisco 2505 router, port numbers range from 1 to 8. On the Cisco 2507 router, port numbers range from 1 to 16. If a second port number follows, this port number indicates the beginning of a port range.
end-port	(Optional) Ending port number of a range.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If you do not specify a port or port range for the **showhub** command, the command displays all ports (for example, ports 1 through 16 on a Cisco 2507 router) by default. Therefore, the **showhub**, **showhubethernet0**, and **showhubethernet0116** commands produce the same result.

If no ports are specified, the command displays some additional data about the internal port. The internal port is the hub's connection to Ethernet interface 0 inside the box. Ethernet interface 0 still exists; physical access to the interface is via the hub.

Examples

Information for a Specific Port

The following is sample output from the **showhub** command for hub 0, port 2 only:

```
Router# show hub ethernet 0 2
Port 2 of 16 is administratively down, link state is down
  0 packets input, 0 bytes
  0 errors with 0 collisions
     (0 FCS, 0 alignment, 0 too long,
      0 short, 0 runts, 0 late,
      0 very long, 0 rate mismatches)
  0 auto partitions, last source address (none)
  Last clearing of "show hub" counters never
```

```
Repeater information (Connected to Ethernet0)
  2792429 bytes seen with 18 collisions, 1 hub resets
  Version/device ID 0/1 (0/1)
  Last clearing of "show hub" counters never
```

Information for All Ports

The following is sample output from the **showhub** command for hub 0, all ports:

```
Router# show hub ethernet 0
Port 1 of 16 is administratively down, link state is up
  2458 packets input, 181443 bytes
  3 errors with 18 collisions
     (0 FCS, 0 alignment, 0 too long,
      0 short, 3 runts, 0 late,
      0 very long, 0 rate mismatches)
  0 auto partitions, last source address was 0000.0cff.e257
  Last clearing of "show hub" counters never
.
.
.
Port 16 of 16 is down, link state is down
  0 packets input, 0 bytes
  0 errors with 0 collisions
     (0 FCS, 0 alignment, 0 too long,
      0 short, 0 runts, 0 late,
      0 very long, 0 rate mismatches)
  0 auto partitions, last source address (none)
  Last clearing of "show hub" counters never

Repeater information (Connected to Ethernet0)
  2792429 bytes seen with 18 collisions, 1 hub resets
  Version/device ID 0/1 (0/1)
  Last clearing of "show hub" counters never

Internal Port (Connected to Ethernet0)
  36792 packets input, 4349525 bytes
  0 errors with 14 collisions
     (0 FCS, 0 alignment, 0 too long,
      0 short, 0 runts, 0 late,
      0 very long, 0 rate mismatches)
  0 auto partitions, last source address (none)
  Last clearing of "show hub" counters never
```

The table below describes significant fields shown in the display.

*Table 110: **show hub** Field Descriptions*

Field	Description
Port ... of ... is administratively down	Port number out of total ports; indicates whether the interface hardware is currently active or down because of the following: • The link-state test failed. • The MAC address mismatched when source address configured. • It has been taken down by an administrator.

Field	Description
link state is up	Indicates whether port has been disabled by the link-test function. If the link-test function is disabled by the user, nothing will be shown here.
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
errors	Sum of FCS, alignment, too long, short, runts, very long, and rate mismatches.
collisions	Number of messages retransmitted due to Ethernet collisions.
FCS	Counter for the number of frames detected on the port with an invalid frame check sequence.
alignment	Counter for the number of frames of valid length (64 to 1518 bytes) that have been detected on the port with an FCS error and a framing error.
too long	Counter for the number of frames that exceed the maximum valid packet length of 1518 bytes.
short	Counter for the number of instances when activity is detected with duration less than 74 to 82 bit times.
runts	Number of packets that are discarded because they are smaller than the medium's minimum packet size. For example, any Ethernet packet that is less than 64 bytes is considered a runt.
late	Counter for the number of instances when a collision is detected after 480 to 565 bit times in the frame.
very longs	Counter for the number of times the transmitter is active in excess of 4 to 7.5 milliseconds.
rate mismatches	Counter for the number of occurrences when the frequency, or data rate of incoming signal is noticeably different from the local transmit frequency.
auto partitions	Counter for the number of instances where the repeater has partitioned the port from the network.
last source address	Source address of last packet received by this port. Indicates "none" if no packets have been received since power on or a hub reset.
Last clearing of "show hub" counters	Elapsed time since the **clearhubcounters** command was entered. Indicates "never" if counters have never been cleared.
Repeater information (Connected to Ethernet0)	Indicates that the following information is about the hub connected to the Ethernet interface shown.
... bytes seen with ... collisions, ... hub resets	Hub resets is the number of times the hub has been reset by network management software or by the **clearhub** command.

Field	Description
Version/device ID 0/1 (0/1)	Hub hardware version. IMR+ version device of daughter board.
Internal Port (Connected to Ethernet0)	Set of counters for the internal AUI port connected to the Ethernet interface.

Related Commands

Command	Description
hub	Enables and configures a port on an Ethernet hub of a Cisco 2505 or Cisco 2507 router.

show hw-module all fpd

To display the current versions of all field-programmable devices (FPDs) for all of the supported card types on a router, enter the **showhw-moduleallfpd** command in privileged EXEC mode.

show hw-module all fpd

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(4)XD	This command was integrated into Cisco IOS Release 12.4(4)XD.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.4(15)T	Added an example for the PA-MC-T3-EC port adapter.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.
Cisco IOS XE Release 3.9S	This command was implemented on Cisco 4400 Series ISRs in Cisco IOS XE Release 3.9S

Usage Guidelines

Other than the FPD version information, the output for this command can also contain useful FPD-related notes.

For more information about FPD upgrades on SPA interface processors (SIPs) and shared port adapters (SPAs), see the Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide.

In Cisco IOS Release 12.2(33)SCB, the FPD image upgrade is supported only for the SPAs inserted in the SIP-600 jacket card on a Cisco uBR10012 router.

Examples

Cisco 7200 VXR

The following example shows an FPD image file version that requires an upgrade (indicated by the asterisk) for the NPE-G2 network processing engine in the Cisco 7200 VXR router:

```
Router# show hw-module all fpd
==== ====================== ====== =============================================
                             H/W    Field Programmable   Current   Min. Required
```

```
Slot Card Type              Ver.  Device: ID-Name    Version      Version
==== ====================== ====== ================== =========== ==============
 npe NPE-G2                 1.5   1-NPEG2 I/O FPGA       0.18         0.20 *
---- ---------------------- ------ ------------------ ----------- --------------
   0 VSA                    0.0   1-VSA                  0.10         0.10
==== ====================== ====== ==============================================
NOTES:
       - FPD images that are required to be upgraded are indicated with a '*'
         character in the Minimal Required Version field.
       - The following FPD image package file is required for the upgrade:
         c7200-fpd-pkg.124-4.XD.pkg
```

The following example shows that all FPDs for the port adapter have the minimum required version. For the NPE-400, the "###" characters in the ID-Name, Current Version, and Min, Required Version fields indicate that FPD does not apply to the NPE-400.

```
Router# show hw-module all fpd
==== ====================== ====== ==============================================
                            H/W   Field Programmable   Current   Min. Required
Slot Card Type              Ver.  Device: ''ID-Name''  Version      Version
==== ====================== ====== ================== =========== ==============
 npe NPE-400                1.1   ############           #.#         #.#
---- ---------------------- ------ ------------------ ----------- --------------
   1 PA-MC-1T3-EC           1.0   1-ToySurprise FPGA     1.2         1.1
                                  2-Subrate FPGA         1.4         1.4
                                  3-Rommon/IPL           2.0         2.0
==== ====================== ====== ==============================================
```

Cisco 7600 Series

The following example shows FPD image file versions for all SIPs and SPAs in the Cisco 7600 series router:

```
Router# show hw-module all fpd
==== ====================== ====== ==============================================
                            H/W   Field Programmable   Current   Min. Required
Slot Card Type              Ver.  Device: ID-Name    Version      Version
==== ====================== ====== ================== =========== ==============
   4 7600-SIP-200           0.132 1-I/O FPGA             0.19        0.18
                                  2-EOS FPGA             0.22        0.22
                                  3-PEGASUS TX FPGA      0.121       0.121
                                  4-PEGASUS RX FPGA      0.13        0.13
                                  5-ROMMON               1.1         1.1
---- ---------------------- ------ ------------------ ----------- --------------
 4/0 SPA-4XOC3-ATM          1.0   1-I/O FPGA             0.121       0.121
---- ---------------------- ------ ------------------ ----------- --------------
 4/1 SPA-8XCHT1/E1          0.117 1-ROMMON               2.12        2.12
                                  2-I/O FPGA             0.22        0.22
---- ---------------------- ------ ------------------ ----------- --------------
 4/3 SPA-4XCT3/DS0          0.253 1-ROMMON               2.12        2.12
                                  2-I/O FPGA             0.21        0.21
                                  3-T3 SUBRATE FPGA      0.15        0.15
==== ====================== ====== ==============================================
```

The following example shows FPD image file versions that require an upgrade (indicated by the asterisk) for two SIPs in the Cisco 7600 series router. The SIPs are disabled due to the version mismatch.

```
Router# show hw-module all fpd
```

```
==== ====================== ====== =============================================
                            H/W    Field Programmable   Current   Min. Required
Slot Card Type              Ver.   Device: ID-Name     Version     Version
==== ====================== ====== ================== =========== ==============
   1 7600-SIP... <DISABLED>  0.550 1-I/O FPGA             1.1         1.1
                                   2-EOS FPGA             1.211       1.211
                                   3-PEGASUS TX FPGA      1.129       1.129
                                   4-PEGASUS RX FPGA      1.3         1.3
                                   5-ROMMON               1.1         1.2     *
---- ---------------------- ------ ------------------ ----------- --------------
   4 7600-SIP... <DISABLED>  0.550 1-I/O FPGA             1.1         1.1
                                   2-EOS FPGA             1.211       1.211
                                   3-PEGASUS TX FPGA      1.129       1.129
                                   4-PEGASUS RX FPGA      1.3         1.3
                                   5-ROMMON               1.1         1.2     *
==== ====================== ====== =============================================
 NOTES:
       - FPD images that are required to be upgraded are indicated with a '*'
         character in the Minimal Required Version field.
       - The following FPD image package file is required for the upgrade:
         c7600-fpd-pkg.122-18.SXE.pkg
```

Cisco uBR10012 Universal Broadband Router

The following example shows the FPD versions on SPAs that meet the minimum requirements in the Cisco uBR10012 router:

```
Router# show hw-module all fpd
==== ====================== ====== =============================================
                            H/W    Field Programmable   Current   Min. Required
Slot Card Type              Ver.   Device: ID-Name    Version      Version
==== ====================== ====== ================== =========== ==============
 1/0 SPA-24XDS-SFP           1.0   1-Modena BLAZE FPG  1285.1444   1285.1444
---- ---------------------- ------ ------------------ ----------- --------------
 1/1 SPA-24XDS-SFP           1.0   1-Modena BLAZE FPG  1285.1444   1285.1444
---- ---------------------- ------ ------------------ ----------- --------------
 1/2 SPA-24XDS-SFP           1.0   1-Modena BLAZE FPG  1285.1444   1285.1444
---- ---------------------- ------ ------------------ ----------- --------------
 1/3 SPA-5X1GE-V2            1.2   1-5xGE V2 I/O FPGA     1.10        1.10
---- ---------------------- ------ ------------------ ----------- --------------
 3/0 SPA-24XDS-SFP           1.0   1-Modena BLAZE FPG  1285.1444   1285.1444
---- ---------------------- ------ ------------------ ----------- --------------
 3/1 SPA-24XDS-SFP           1.0   1-Modena BLAZE FPG  1285.1444   1285.1444
---- ---------------------- ------ ------------------ ----------- --------------
 3/2 SPA-24XDS-SFP           1.0   1-Modena BLAZE FPG  1285.1444   1285.1444
---- ---------------------- ------ ------------------ ----------- --------------
 3/3 SPA-1X10GE-L-V2         1.2   1-10GE V2 I/O FPGA     1.9         1.9
==== ====================== ====== =============================================
```

Example: Cisco 4400 Series ISRs

will be added later

Related Commands

Command	Description
show hw-module slot fpd	Displays the current versions of all FPDs for a SIP in the specified slot location and for all of the SPAs installed in that SIP or any FPD-capable cards.
show hw-module subslot fpd	Displays the current versions of all FPDs for a particular SPA or all of the active SPAs on a router.

show hw-module slot (6500)

To display information for a SPA interface processor (SIP) or a module, use the **showhw-moduleslot** command in privileged EXEC configuration mode.

show hw-module slot *slot* {**clear-block** | **oversubscription** | **port-group-mapping**}

Syntax Description

slot	Specifies the chassis slot number. See the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide.
clear-block	Displays the clearing of the head-of-line blocking status.
oversubscription	Displays the oversubscription mode of each port-group.
port-group-mapping	Displays the port group mapping.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXF5	Support for this command was introduced (Catalyst 6500 series switch).
12.(33)SXH1	This command was changed to add the **oversubscription** and the **port-group-mapping** keywords (Catalyst 6500 series switch).
12.2(33)SXH2	This command was changed to support the following modules: • WS-X6716-10G-3C • WS-X6716-10G-3CXL

Usage Guidelines

This command is supported on the following modules:

- WS-X6708-10G-3C--The port-group**mapping** and the clear-block keywords are not supported.
- WS-X6708-10G-3CXL--The port-group *num* and the clear-block keywords and argument are not supported.
- WS-X6716-10G-3C
- WS-X6716-10G-3CXL

The port-group mappings for the WS-X6716-10G-3C and the WS-X6716-10G-3CXL modules are as follows:

- Group 1--Ports 1 to 4. Port 1 is enabled in transparent mode.
- Group 2--Ports 5 to 8. Port 5 is enabled in transparent mode.
- Group 3--Ports 9 to 12. Port 9 is enabled in transparent mode.

- Group 4--Ports 13 to 16. Port 13 is enabled in transparent mode.

For the WS-X6716-10G-3C and the WS-X6716-10G-3CXL modules in transparent mode, ports 2, 3, 4, 6, 7, 8, 10, 11, 12, 14, 15, 16 are disabled.

Examples

This example shows how to display the current configuration status for the four port-groups:

```
Router# show hw-module slot 2 clear-block
Port-group Clear-block
1          Enabled
2          Disabled
3          Disabled
4          Enabled
Router#
```

This example shows how to display the port group mapping of each port group:

```
Router# show hw-module slot 2 port-group-mapping
Port-group Ports
1          1, 2, 3, 4
2          5, 6, 7, 8
3          9, 10, 11, 12
4          13, 14, 15, 16
```

This example shows how to display the oversubscription mode of each port group:

```
Router# show hw-module slot 3 oversubscription
Port-group oversubscription mode
1          Enabled
2          Disabled
3          Enabled
4          Disabled
Router#
```

Related Commands

Command	Description
hw-module oversubscription	Administratively enables or disables the oversubscribed ports on a module.

show hw-module slot align

To display alignment data for a SPA interface processor (SIP) or other module, use the **showhw-moduleslotalign** command in privileged EXEC configuration mode.

show hw-module slot *slot* **align** [**cpu** {**0** | **1**}]

Syntax Description

slot	Chassis slot number. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide.
cpu 0 |**1**	(Optional) Number of the CPU (0 or 1) for which you want to display data.

Command Default

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	Thiscommand was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The number of CPUs available varies by the type of SIP. Although the Cisco 7600 SIP-200 has two CPUs, you can display alignment data for the first CPU (CPU 0) only.

Examples

The following example shows that there has not been any alignment data for the SIP installed in slot 2 of the router:

```
Router# show hw-module slot 2 align
No alignment data has been recorded.
No spurious memory references have been recorded.
```

show hw-module slot fpd

To display the current versions of all field-programmable devices (FPDs) for a SIP in the specified slot location and for all of the SPAs installed in that SIP, or to display the current versions of any FPD-capable cards, enter the **showhw-moduleslotfpd** command in privileged EXEC mode.

Cisco 7200 VXR
show hw-module slot {*slot* | **npe**} **fpd**

Cisco 7304, Cisco 7600 Series, Cisco 12000 Series
show hw-module slot *slot* **fpd**

Syntax Description

slot	Chassis slot number. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding “Identifying Slots and Subslots for SIPs and SPAs” topic in the platform-specific SPA software configuration guide. For slot numbering in the Cisco 7200 VXR router, refer to the Cisco 7200 VXR Installation and Configuration Guide .
npe	NPE-G2 network processing engine in the Cisco 7200 VXR router.

Command Default

No default behavior or values

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(4)XD	This command was integrated into Cisco IOS Release 12.4(4)XD, and the npe keyword was added.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

Use the **showhw-moduleslotfpd** command to show the FPD image version information for a particular SIP and all of its installed SPAs, or to display the current versions of FPD-capable cards in the Cisco 7200 VXR router. To display FPD information for all of the supported card types on a router, use the **showhw-moduleallfpd** command.

Other than the FPD version information, the output for this command can also contain useful FPD-related notes.

For more information about FPD upgrades on SPA interface processors (SIPs) and shared port adapters (SPAs), see the Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide.

Examples

Cisco 7200 VXR

The following example shows that the FPD version on the NPE-G2 meets the minimum FPD version requirements:

```
Router# show hw-module slot npe fpd
==== =================== ====== =============================================
                             H/W   Field Programmable   Current   Min. Required
Slot Card Type               Ver.  Device: "ID-Name"    Version      Version
==== =================== ====== ================== =========== ==============
 npe NPE-G2                  1.3   1-NPEG2 I/O FPGA       0.19        0.1
==== =================== ====== =============================================
```

The following example shows FPD information for the VPN Services Adapter (VSA) in slot 0:

```
Router# show hw-module slot 0 fpd
==== =================== ====== =============================================
                             H/W   Field Programmable   Current   Min. Required
Slot Card Type               Ver.  Device: "ID-Name"    Version      Version
==== =================== ====== ================== =========== ==============
   0 VSA                     0.0   1-VSA                  0.9         0.8
==== =================== ====== =============================================
```

Cisco 7600 Series

The following example shows that the FPD versions on the SIP installed in chassis slot 4, and each of its installed SPAs, meet the minimum FPD version requirements:

```
Router# show hw-module slot 4 fpd
==== ====================== ====== =============================================
                                H/W   Field Programmable   Current   Min. Required
Slot Card Type                  Ver.  Device: "ID-Name"    Version      Version
==== ====================== ====== ================== =========== ==============
   4 7600-SIP-200               0.550 1-I/O FPGA             1.1         1.1
                                      2-EOS FPGA             1.211       1.211
                                      3-PEGASUS TX FPGA      1.129       1.129
                                      4-PEGASUS RX FPGA      1.3         1.3
                                      5-ROMMON               1.2         1.2
---- ---------------------- ------ ------------------ ----------- --------------
 4/0 SPA-2XT3/E3                1.0   1-ROMMON               2.12        2.12
                                      2-I/O FPGA             0.24        0.24
                                      3-E3 FPGA              0.6         0.6
                                      4-T3 FPGA              0.14        0.14
---- ---------------------- ------ ------------------ ----------- --------------
 4/1 SPA-4XOC3-POS              0.209 1-I/O FPGA             3.4         3.4
---- ---------------------- ------ ------------------ ----------- --------------
 4/2 SPA-8XCHT1/E1              0.117 1-ROMMON               2.12        2.12
                                      2-I/O FPGA             1.2         1.2
==== ====================== ====== =============================================
```

Related Commands

Command	Description
show hw-module all fpd	Displays the current versions of all FPDs for all of the supported card types on a router.

Command	Description
show hw-module subslot fpd	Displays the current versions of all FPDs for a particular SPA or all of the active SPAs on a router.

show hw-module slot logging

To display logging information for a SPA interface processor (SIP) or other module, use the **showhw-moduleslotlogging** command in privileged EXEC configuration mode.

show hw-module slot *slot* **logging** [**cpu** {**0** | **1**}]

Syntax Description

slot	Chassis slot number. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide.
cpu 0 |**1**	(Optional) Number of the CPU (0 or 1) for which you want to display data.

Command Default

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	Thiscommand was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The number of CPUs available varies by the type of SIP. Although the Cisco 7600 SIP-200 has two CPUs, you can display alignment data for the first CPU (CPU 0) only.

Examples

The following example shows logging information and messages for the SIP installed in slot 2 of the router:

```
Router# show hw-module slot 2 logging
Syslog logging: enabled (0 messages dropped, 2 messages rate-limited, 0 flushes,
 0 overruns)
    Console logging: level debugging, 90 messages logged
    Monitor logging: level debugging, 0 messages logged
    Buffer logging: level debugging, 92 messages logged
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
Log Buffer (8192 bytes):
00:00:01:  hyp_dev_attach
00:00:01:  hyp_dev_init
00:00:01:  hyp_init
00:00:01:  hyp_dev_disable_intr
00:00:01:  hyp_mx_sub_core_reset
00:00:01:  hyp_mx_sub_core_unreset
00:00:01:  hyp_mx_slv_reset
00:00:01:  hyp_mx_slv_unreset
00:00:01:  hyp_reg_config
00:00:01:  hyp_fi_fr_reg_config
00:00:01:  hyp_set_oper_mode
00:00:01:  hyp_dev_enable_intr
00:00:03:  Initializing rate limit function ===!!!
```

```
00:00:04: Currently running ROMMON from ROM F2
SLOT 2/0: 00:00:04: %SYS-5-RESTART: System restarted --
Cisco Internetwork Operating System Software
IOS (tm) cwlc Software (sip1-DW-M), Experimental Version 12.2(20040824:180829) [
dperez-pikespeak_3 174]
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Wed 01-Sep-04 13:54 by dperez
00:00:05:  hyp_init
00:00:05:  hyp_dev_disable_intr
00:00:05:  hyp_mx_sub_core_reset
00:00:05:  hyp_mx_sub_core_unreset
00:00:05:  hyp_mx_slv_reset
00:00:05:  hyp_mx_slv_unreset
00:00:05:  hyp_reg_config
00:00:05:  hyp_fi_fr_reg_config
00:00:05:  hyp_set_oper_mode
00:00:05:  hyp_dev_enable_intr
SLOT 2/0: 00:00:05: %HYPERION-5-BUS_MODE_CHANGE: The System Switching Bus Mode c
hanged to Compact mode
00:00:05:
00:00:05:  hyp_fabric_intf_cnfg
00:00:05: Fabric Information
00:00:05: ==================
00:00:05:  Speed        = 8G
00:00:05:  Channel mode = Mode2-SSA/SSO
00:00:05:  Channel      = Secondary
00:00:05:  hyp_rbh_reg_clear
00:00:05:  Serial Secondary Channel SYNC SUCCESS!
SLOT 2/0: 00:00:05: %SCP-5-ENABLE: Module enabled
00:00:05:  hyp_fabric_intf_cnfg
00:00:05:  hyp_fpoe_chan_init
00:00:05: sip_hyp_check_sync_100ms:Opened SSA DDR
00:00:05: sip_hyp_check_sync_100ms:Opened n/w DDR
SLOT 2/0: 00:00:08: %SCP-5-ONLINE: Module online
00:00:09: % FPD_MGMT[65535]: Sending FPD version check request
00:00:09: % FPD_MGMT[65535]: Change FPD upgrade state to FPD_STATE_UPGRADE_IN_PR
OGRESS
00:00:09: % FPD_MGMT[65535]: Change FPD upgrade state to FPD_STATE_NO_UPGRADE_NE
EDED
SLOT 2/0: 00:00:09: %SIPSPA-6-OIR: Bay 3 SPA Power changed to On
SLOT 2/0: 00:00:10: %SIPSPA-6-OIR: Bay 3 SPA OK changed to On
00:00:10: % FPD_MGMT[3]: Sending FPD version check request
00:00:10: % FPD_MGMT[3]: Change FPD upgrade state to FPD_STATE_UPGRADE_IN_PROGRE
SS
00:00:10: % FPD_MGMT[3]: Change FPD upgrade state to FPD_STATE_NO_UPGRADE_NEEDED
SLOT 2/0: 00:00:13: %SCC-2-PROTO_HW: Module (2/3) is a registered proto-type for
 Cisco Lab use only, and not certified for live network operation.
SLOT 2/0: 00:00:15: %LINK-3-UPDOWN: Interface POS2/3/0, changed state to down
```

show hw-module slot proc cpu

To display CPU utilization for each process on a SPA interface processor (SIP) or other module, use the **showhw-moduleslotproccpu**command in privileged EXEC configuration mode.

show hw-module slot *slot* **proc cpu** [**cpu** {**0** | **1**}]

Syntax Description

slot	Chassis slot number. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding “Identifying Slots and Subslots for SIPs and SPAs” topic in the platform-specific SPA software configuration guide.
cpu 0 |1	(Optional) Number of the CPU (0 or 1) for which you want to display data.

Command Default

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	Thiscommand was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The number of CPUs available varies by the type of SIP. Although the Cisco 7600 SIP-200 has two CPUs, you can display alignment data for the first CPU (CPU 0) only.

Examples

The following example shows CPU utilization per process for the SIP installed in slot 2 of the router:

```
Router# show hw-module slot 2 proc cpu
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           0         1          0  0.00%  0.00%  0.00%   0 Chunk Manager
   2           0    255569          0  0.00%  0.00%  0.00%   0 Load Meter
   3           4   1884015          0  0.00%  0.00%  0.00%   0 CEF process
   4       86532    129737        666  0.08%  0.00%  0.00%   0 Check heaps
   5           0       743          0  0.00%  0.00%  0.00%   0 Pool Manager
   6           0         2          0  0.00%  0.00%  0.00%   0 Timers
   7           0         1          0  0.00%  0.00%  0.00%   0 AAA_SERVER_DEADT
   8           0         2          0  0.00%  0.00%  0.00%   0 AAA high-capacit
   9           0         2          0  0.00%  0.00%  0.00%   0 Serial Backgroun
  10           0    255598          0  0.00%  0.00%  0.00%   0 ENVM Background
  11           0     21298          0  0.00%  0.00%  0.00%   0 IPC Dynamic Cach
  12          56     21300          2  0.00%  0.00%  0.00%   0 PROCMIB LC Proce
  13           0         1          0  0.00%  0.00%  0.00%   0 IPC BackPressure
  14           0   1277836          0  0.00%  0.00%  0.00%   0 IPC Periodic Tim
  15           0   1277836          0  0.00%  0.00%  0.00%   0 IPC Deferred Por
  16           0        13          0  0.00%  0.00%  0.00%   0 IPC Seat Manager
  17           0         1          0  0.00%  0.00%  0.00%   0 SERIAL A'detect
  18        2820        39      72307  0.00%  0.00%  0.00%   0 SMART
  19           0         1          0  0.00%  0.00%  0.00%   0 Critical Bkgnd
  20           4    383354          0  0.00%  0.00%  0.00%   0 Net Background
```

```
21          0        36          0  0.00%  0.00%  0.00%   0 Logger
22          8   1277832          0  0.00%  0.00%  0.00%   0 TTY Background
23          0   1277846          0  0.00%  0.00%  0.00%   0 Per-Second Jobs
24          0     22041          0  0.00%  0.00%  0.00%   0 Per-minute Jobs
25          0         2          0  0.00%  0.00%  0.00%   0 SCP Multicast
26          0         1          0  0.00%  0.00%  0.00%   0 Inode Table Dest
27          0         4          0  0.00%  0.00%  0.00%   0 LC to RP  defere
28          8       428         18  0.00%  0.00%  0.00%   0 CWLC IFCOM Proce
29          0         1          0  0.00%  0.00%  0.00%   0 IPC RTTYC Messag
30          0         2          0  0.00%  0.00%  0.00%   0 INTR MGR PROCESS
31          0         2          0  0.00%  0.00%  0.00%   0 EFC queue monito
32          0         1          0  0.00%  0.00%  0.00%   0 LC interrupt, J1
33          0         1          0  0.00%  0.00%  0.00%   0 SIP interrupt, P
34          0         2          0  0.00%  0.00%  0.00%   0 SDCC Input
35          0         1          0  0.00%  0.00%  0.00%   0 CWAN LTL manager
36          0         8          0  0.00%  0.00%  0.00%   0 SIP SWBus Sync P
37          0         1          0  0.00%  0.00%  0.00%   0 CWSLC Bus Stall
38          0         1          0  0.00%  0.00%  0.00%   0 VIP Encap IPC Ba
39          0         1          0  0.00%  0.00%  0.00%   0 CWPA Bridging Ra
40          0    255568          0  0.00%  0.00%  0.00%   0 CPU Monitor
41          0         1          0  0.00%  0.00%  0.00%   0 MLP Input
42        592     42648         13  0.00%  0.00%  0.00%   0 SPA OIR 2/0
43        644     42644         15  0.00%  0.00%  0.00%   0 SPA OIR 2/1
44        572     42644         13  0.00%  0.00%  0.00%   0 SPA OIR 2/2
45       1088     42697         25  0.00%  0.00%  0.00%   0 SPA OIR 2/3
46          0         1          0  0.00%  0.00%  0.00%   0 LC FPD Upgrade P
47          0         2          0  0.00%  0.00%  0.00%   0 AAA Dictionary R
48          0         2          0  0.00%  0.00%  0.00%   0 AAA Server
49          0         1          0  0.00%  0.00%  0.00%   0 AAA ACCT Proc
50          0         1          0  0.00%  0.00%  0.00%   0 ACCT Periodic Pr
51          0         2          0  0.00%  0.00%  0.00%   0 ATMLS task
52          0    127785          0  0.00%  0.00%  0.00%   0 LC Process for u
53          0         3          0  0.00%  0.00%  0.00%   0 IP Hdr Comp Proc
54        140  12778349          0  0.00%  0.00%  0.00%   0 SSA FABLINK Proc
55          0    255568          0  0.00%  0.00%  0.00%   0 HYP ACCU FAB COU
56          0         1          0  0.00%  0.00%  0.00%   0 SCP async: CWAN-
57          0         2          0  0.00%  0.00%  0.00%   0 CWTLC SSO Proces
58       3272     85294         38  0.00%  0.00%  0.00%   0 SCP Hybrid proce
59       1004  12717003          0  0.00%  0.00%  0.00%   0 CEF LC IPC Backg
60          8   1653487          0  0.00%  0.00%  0.00%   0 CEF LC Stats
61          0         1          0  0.00%  0.00%  0.00%   0 CEF MQC IPC Back
62          0         1          0  0.00%  0.00%  0.00%   0 TFIB LC cleanup
63          0         3          0  0.00%  0.00%  0.00%   0 Any Transport ov
64          0         7          0  0.00%  0.00%  0.00%   0 HQF Shaper Backg
65          8 319458609          0  0.00%  0.00%  0.00%   0 HQF Input Shaper
66          0         2          0  0.00%  0.00%  0.00%   0 LOCAL AAA
67          0         2          0  0.00%  0.00%  0.00%   0 AAA Cached Serve
68          0     90366          0  0.00%  0.00%  0.00%   0 CEF Scanner
69          0         3          0  0.00%  0.00%  0.00%   0 RADIUS TEST CMD
70          0         2          0  0.00%  0.00%  0.00%   0 AAA SEND STOP EV
71          0         4          0  0.00%  0.00%  0.00%   0 IPv6 CEF process
72          0         1          0  0.00%  0.00%  0.00%   0 SONET alarm time
73          0         1          0  0.00%  0.00%  0.00%   0 Net Input
74          0    255571          0  0.00%  0.00%  0.00%   0 Compute load avg
75         16        80        200  0.08%  0.00%  0.00%   1 console_rpc_serv
```

show hw-module slot tech-support through show interfaces vg-anylan

show hw-module slot tech-support

To display system information for a SPA interface processor (SIP) or other module to troubleshoot a problem, use the **showhw-moduleslottech-support**command in privileged EXEC configuration mode.

show hw-module slot *slot* **tech-support** [**cpu** {**0** | **1**}]

Syntax Description

slot	Chassis slot number. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding “Identifying Slots and Subslots for SIPs and SPAs” topic in the platform-specific SPA software configuration guide.
cpu 0 |1	(Optional) Number of the CPU (0 or 1) for which you want to display data.

Command Default

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	Thiscommand was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **showhw-moduleslottech-support** command to gather information about the SIP or other module to troubleshoot a problem. Certain error messages request that you gather this information and have it available when reporting a problem to Cisco Systems technical support personnel.

The **showhw-moduleslottech-support**command runs a collection of different **show** commands to gather information about your system environment and configuration.

The number of CPUs available varies by the type of SIP. Although the Cisco 7600 SIP-200 has two CPUs, you can display alignment data for the first CPU (CPU 0) only.

Examples

The following example shows system information for the SIP installed in slot 5 of the router:

```
Router# show hw-module slot 5 tech-support
------------------ show version ------------------
Cisco Internetwork Operating System Software
IOS (tm) cwlc Software (sip2-DW-M), Version 12.2(PIKESPEAK_INTEG_041013) INTERIM SOFTWARE
Synced to V122_18_S6, 12.2(18)S6 on v122_18_s_throttle, Weekly 12.2(18.6.4)SX
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Wed 13-Oct-04 06:55 by kchristi
Image text-base: 0x40010FC0, data-base: 0x40680000
ROM: System Bootstrap, Version 12.2(20040716:151531) [tawei-pike1 1.1dev(0.1)] DEVELOPMENT
 SOFTWARE
ROM: cwlc Software (sip2-DW-M), Version 12.2(PIKESPEAK_INTEG_041013) INTERIM SOFTWARE
SIP-400-5 uptime is 19 hours, 38 minutes
System returned to ROM by power-on
Running default software
```

```
cisco CWAN Modular Service Card (SIP-400) (SB-1) processor with 245760K/16383K bytes of
memory.
SB-1 CPU at 400Mhz, Implementation 0x401, Rev 0.3, 256KB L2 Cache
Last reset from power-on
4 ATM network interface(s)
Configuration register is 0x0
------------------ show running-config ------------------
Building configuration...
Current configuration : 13 bytes
!
!
!
!
end
------------------ show stacks ------------------
Minimum process stacks:
 Free/Size   Name
 5080/6000   SCP Find Master process
 8448/12000  Init
 5528/6000   IPC Zone Manager
 5264/6000   SCP Hybrid Registration process
 4616/6000   IPC delayed init
 5056/6000   SIP2 FPD Process
 8120/12000  Exec
 6920/12000  console_rpc_server_action
 7536/12000  RFSS_server_action
Interrupt level stacks:
Level    Called Unused/Size  Name
  1           1   7896/9000  Level 1 Interrupt
  2      116555   6136/9000  Level 2 Interrupt
  3         289   7760/9000  Level 3 Interrupt
  4       24915   8392/9000  Level 4 Interrupt
  5          67   8424/9000  Level 5 Interrupt
  7    17683668   8568/9000  NMI Interrupt Handler
------------------ show interfaces ------------------
ATM5/0/0 is administratively down, line protocol is down
  Hardware is SPA-4XOC3-ATM, address is 0000.0000.0000 (bia 0000.0000.0000)
  MTU 4470 bytes, sub MTU 0, BW 149760 Kbit, DLY 0 usec,
     reliability 0/255, txload 1/255, rxload 1/255
  Encapsulation ATM, loopback not set
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
ATM5/0/1 is administratively down, line protocol is down
  Hardware is SPA-4XOC3-ATM, address is 0000.0000.0000 (bia 0000.0000.0000)
  MTU 4470 bytes, sub MTU 0, BW 149760 Kbit, DLY 0 usec,
     reliability 0/255, txload 1/255, rxload 1/255
  Encapsulation ATM, loopback not set
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
```

```
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
ATM5/0/2 is administratively down, line protocol is down
  Hardware is SPA-4XOC3-ATM, address is 0000.0000.0000 (bia 0000.0000.0000)
  MTU 4470 bytes, sub MTU 0, BW 149760 Kbit, DLY 0 usec,
     reliability 0/255, txload 1/255, rxload 1/255
  Encapsulation ATM, loopback not set
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
ATM5/0/3 is administratively down, line protocol is down
  Hardware is SPA-4XOC3-ATM, address is 0000.0000.0000 (bia 0000.0000.0000)
  MTU 4470 bytes, sub MTU 0, BW 149760 Kbit, DLY 0 usec,
     reliability 0/255, txload 1/255, rxload 1/255
  Encapsulation ATM, loopback not set
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
------------------ show controllers ------------------
Shared Port Adapter SPA-4XOC3-ATM[5/0]
 4xOC3 ATM SPA revision 1
SAR is Azanda Katana SAR/TM, rev B, manf_id 0x1B2, base 0xB8300000
 object     0x43D9DF90, port      0x43A332E8, list_elems 0x43A3C7D0
 hash_tbl   0x41EEF0A0, vc_tbl    0x4276C2F0, fid_tbl    0x441145A0
 shp_prof   0x42996990
 vc_count 0/16384 (curr/max), fid_count 12/65536 (curr/max), max_bids 1048576
 Device level stats:
  s4p3_abort                 0  s4p3_pty_errs              0
  cor_ecc_errs               0  lut_pty_errs               0
  uncor_ecc_errs             0  hdrap_pty_errs             0
  mem_bad_errs               0
  pfq2mem_rels               0  null_rel                   0
  mem2pfq_rels               0  null_dq                    0
  mem_nq                     0  pre_pfq_drops              0
  dbs_dq_cnt                 0  post_pfq_drops             0
```

```
  no_fid_drops               0  tot_free_bufs       1048575
  bid_nulls                  0  bufs_inuse                0
  sch_cells                  0  sch_cells_out             0
  sch_blocked                0  sch_eop                   0
  sch_empty                  0  cbwfq_merge_in            0
  cbwfq_merge_out            0
Backpressure status:
 SEG input FIFO: not full
            LUT    RAS    PFQ    DBS
           lo hi  lo hi  lo hi  lo hi
 Port 0 RX  -  -   -  -   -  -   -  -
 Port 0 TX  -  -   -  -   -  -   -  -
 Port 1 RX  -  -   -  -   -  -   -  -
 Port 1 TX  -  -   -  -   -  -   -  -
 Port 2 RX  -  -   -  -   -  -   -  -
 Port 2 TX  1  1   -  -   -  -   -  -
 Port 3 RX  -  -   -  -   -  -   -  -
 Port 3 TX  1  1   -  -   -  -   -  -
 Port 0 Stats:
  rx_paks                    0  tx_paks                   0
  rx_cells                   0  tx_cells                  0
  rx_bytes                   0  tx_bytes                  0
  pm_rx_paks                 0  pm_tx_paks                0
  pm_rx_bytes                0  pm_tx_bytes               0
  rx_wred_tail_dr            0  tx_wred_tail_dr           0
  rx_wred_prob_dr            0  tx_wred_prob_dr           0
  rx_buf_thr_lo          62260  tx_buf_thr_lo        186778
  rx_bufs_inuse_l            0  tx_bufs_inuse_l           0
  rx_buf_thr_hi           3276  tx_buf_thr_hi          9830
  rx_bufs_inuse_h            0  tx_bufs_inuse_h           0
  rx_crc32_errs              0  rx_crc10_errs             0
  rx_no_vcd                  0
 Port 1 Stats:
  rx_paks                    0  tx_paks                   0
  rx_cells                   0  tx_cells                  0
  rx_bytes                   0  tx_bytes                  0
  pm_rx_paks                 0  pm_tx_paks                0
  pm_rx_bytes                0  pm_tx_bytes               0
  rx_wred_tail_dr            0  tx_wred_tail_dr           0
  rx_wred_prob_dr            0  tx_wred_prob_dr           0
  rx_buf_thr_lo          62260  tx_buf_thr_lo        186778
  rx_bufs_inuse_l            0  tx_bufs_inuse_l           0
  rx_buf_thr_hi           3276  tx_buf_thr_hi          9830
  rx_bufs_inuse_h            0  tx_bufs_inuse_h           0
  rx_crc32_errs              0  rx_crc10_errs             0
  rx_no_vcd                  0
 Port 2 Stats:
  rx_paks                    0  tx_paks                   0
  rx_cells                   0  tx_cells                  0
  rx_bytes                   0  tx_bytes                  0
  pm_rx_paks                 0  pm_tx_paks                0
  pm_rx_bytes                0  pm_tx_bytes               0
  rx_wred_tail_dr            0  tx_wred_tail_dr           0
  rx_wred_prob_dr            0  tx_wred_prob_dr           0
  rx_buf_thr_lo          62260  tx_buf_thr_lo        186778
  rx_bufs_inuse_l            0  tx_bufs_inuse_l           0
  rx_buf_thr_hi           3276  tx_buf_thr_hi          9830
  rx_bufs_inuse_h            0  tx_bufs_inuse_h           0
  rx_crc32_errs              0  rx_crc10_errs             0
  rx_no_vcd                  0
 Port 3 Stats:
  rx_paks                    0  tx_paks                   0
  rx_cells                   0  tx_cells                  0
  rx_bytes                   0  tx_bytes                  0
```

```
  pm_rx_paks                 0  pm_tx_paks                 0
  pm_rx_bytes                0  pm_tx_bytes                0
  rx_wred_tail_dr            0  tx_wred_tail_dr            0
  rx_wred_prob_dr            0  tx_wred_prob_dr            0
  rx_buf_thr_lo          62260  tx_buf_thr_lo         186778
  rx_bufs_inuse_l            0  tx_bufs_inuse_l            0
  rx_buf_thr_hi           3276  tx_buf_thr_hi           9830
  rx_bufs_inuse_h            0  tx_bufs_inuse_h            0
  rx_crc32_errs              0  rx_crc10_errs              0
  rx_no_vcd                  0
 Flow utilization summary
          blks  unsh  t_rt  t_lb  t_lf  rt_lf  shap  root  drain | Total
  # free : 24568 0     1023  8184  0     8191  15355 8191   0     | 65512
flow                 int     red dfl    queue size         sent          packet drops
 id   vcd  gqid use  prt dir pro clr curr  avg     max     paks    bufm  giant to/ab pl/crc
0001     0 0000 shap  1  tx   18  4      0     1   35940        0      0     0     0     0
0002     0 0000 shap  3  tx   18  4      0     1   35940        0      0     0     0     0
0003     0 0000 shap  5  tx   18  4      0     1   35940        0      0     0     0     0
0004     0 0000 shap  7  tx   18  4      0     1   35940        0      0     0     0     0
FFF8     0 0000 unsh 11  rx   18  4      0     1   35940        0      0     0     0     0
FFF9     0 0000 unsh 13  rx   18  4      0     1   35940        0      0     0     0     0
FFFA     0 0000 unsh 15  rx   18  4      0     1   35940        0      0     0     0     0
FFFB     0 0000 unsh 17  rx   18  4      0     1   35940        0      0     0     0     0
FFFC     0 0000 unsh 10  rx   21  0      0     1       0        0      0     0     0     0
FFFD     0 0000 unsh 12  rx   21  0      0     1       0        0      0     0     0     0
FFFE     0 0000 unsh 14  rx   21  0      0     1       0        0      0     0     0     0
FFFF     0 0000 unsh 16  rx   21  0      0     1       0        0      0     0     0     0
KATM FPGA: rev 0.90, base 0xB8000000, obj 0x42994748
            packets                cells                 errors
port     rx         tx         rx         tx         rx         tx
 0          0          0          0          0          0          0
 1          0          0          0          0          0          0
 2          0          0          0          0          0          0
 3          0          0          0          0          0          0
PM5379 ATM Framer: Type:0, Rev:1, base 0xB8100000, obj 0x41EEA2B0
                    Cells                   CRC errs
port          rx               tx              rx
0             0                0               0
1             0                0               0
2             0                0               0
3             0                0               0
ATM5/0/0:
        ID: SFP
        Extended ID: 4
        Xcvr Type: OC3 SR-1/STM1 MM (1)
        Connector: LC
        Vendor name: OCP
        Product Identifier (PID): TRP-03BCS
        State: Enabled
ATM5/0/0:
Phased Initialization
        Phase Reached: 4
        Phase Exit Code: Success 0
        Phase Read Offset: 256
Socket Verification
        Compatibility: Compatibility passed
        Security: Security passed
------------------ show memory statistics ------------------
                Head    Total(b)     Used(b)     Free(b)   Lowest(b)  Largest(b)
Processor   4145B860   230311840   118715296   111596544   106212312    48534600
      I/O    F000000    16776736     3090304    13686432    13686432    13685880
------------------ show process memory ------------------
Total: 247088544, Used: 121805424, Free: 125283120
 PID TTY  Allocated      Freed    Holding    Getbufs    Retbufs Process
```

```
   0   0   17899632      57040   17017720          0          0 *Init*
   0   0       1256     145000       1256          0          0 *Sched*
   0   0          0          0          0          0          0 *Neutrino*
   0   0    5233000    4617848     589152     606508          0 *Dead*
   1   0          0          0       6968          0          0 Chunk Manager
   2   0        192        192       3960          0          0 Load Meter
   3   0          0          0       6960          0          0 SCP async: CWAN-
   4   0          0          0       6960          0          0 Check heaps
   5   0      25984     169280       9584      15748      51748 Pool Manager
   6   0        192        192       6960          0          0 Timers
   7   0          0          0       6976          0          0 AAA_SERVER_DEADT
   8   0        192        192       6968          0          0 AAA high-capacit
   9   0        192        192       6960          0          0 Serial Backgroun
  10   0          0          0       6960          0          0 ENVM Background
  11   0          0          0       6960          0          0 IPC Dynamic Cach
  12   0     145256        384      23968      31200          0 PROCMIB LC Proce
  13   0          0          0       6960          0          0 IPC BackPressure
  14   0       7040          0       6960          0          0 IPC Periodic Tim
  15   0          0          0       6968          0          0 IPC Deferred Por
  16   0     123536        352      25416      12756          0 IPC Seat Manager
  17   0          0          0       6960          0          0 SERIAL A'detect
  18   0     992944     993024       6960          0          0 SMART
  19   0          0          0       6960          0          0 Critical Bkgnd
  20   0      14080          0      13120          0          0 Net Background
  21   0        192        192      12960          0          0 Logger
  22   0      26384        448       9960          0          0 TTY Background
  23   0          0          0       6960          0          0 Per-Second Jobs
  24   0          0          0       6960          0          0 Per-minute Jobs
  25   0          0        152       6960          0          0 SCP Multicast
  26   0          0          0       3960          0          0 Inode Table Dest
  27   0          0          0       6976          0          0 LC to RP  defere
  28   0        192        192       6960          0          0 CWLC IFCOM Proce
  29   0          0          0       6968          0          0 IPC RTTYC Messag
  30   0        192        192      12960          0          0 INTR MGR PROCESS
  31   0          0          0       6960          0          0 ixp_exmem_reuse_
  32   0      14456      14296       7120          0          0 spnpc_dowork
  33   0          0          0       6960          0          0 Spi4 Timer
  34   0          0          0       6968          0          0 LC interrupt, J1
  35   0          0          0       6976          0          0 SIP interrupt, P
  36   0          0          0      12960          0          0 SDCC Input
  37   0        192        192      12960          0          0 SDCC Periodic
  38   0        192        192      12960          0          0 SDCC IO
  39   0          0          0       6960          0          0 CWAN LTL manager
  40   0          0          0       6960          0          0 msg_handler_proc
  41   0    2620112    2620112       6960          0          0 Cardmgr Periodic
  42   0          0          0       6960          0          0 SIP SWBus Sync P
  43   0          0          0       6960          0          0 NP doorbell proc
  44   0      10432       5344       6960       2268          0 CardMgr Events
  45   0    1905448       3592    1787560          0          0 INP Reload
  46   0          0          0       6960          0          0 ipc_handler_proc
  47   0          0          0       6960          0          0 NP doorbell proc
  48   0    2270440       2328    2158576       2268          0 ENP Reload
  49   0          0          0       6960          0          0 ipc_handler_proc
  50   0          0          0       6960          0          0 SIP2 Bus Stall
  51   0 1504729392 1504768488     200528          0          0 ifnpc_dowork
  52   0          0          0       6960          0          0 hmi_dowork
  53   0       7000       7000       6960          0          0 cwanlc_npc_dowor
  54   0          0          0       6968          0          0 VIP Encap IPC Ba
  55   0  554366168  457784816   96580296      12756          0 SPA OIR 5/0
  56   0          0          0      12960          0          0 SPA OIR 5/1
  57   0          0          0      12960          0          0 SPA OIR 5/2
  58   0          0          0      12960          0          0 SPA OIR 5/3
  59   0   27281752   27281752       6960          0          0 LC FPD Upgrade P
  60   0          0          0       6960          0          0 spa_env_monitor
```

```
  61  0        192        192       6960          0          0 AAA Dictionary R
  62  0        192        192       6960          0          0 AAA Server
  63  0          0          0       6960          0          0 AAA ACCT Proc
  64  0          0          0       6960          0          0 ACCT Periodic Pr
  65  0        192        192       6960          0          0 ATMLS task
  66  0          0          0       6968          0          0 AToM NP CLIENT B
  67  0          0          0       6968          0          0 TTFIB NP CLIENT
  68  0          0          0       6960          0          0 SSA FABLINK Proc
  69  0          0          0       6968          0          0 HYP ACCU FAB COU
  70  0     327264          0     327264          0          0 CEF process
  71  0        192        192       6960          0          0 CWTLC SSO Proces
  72  0        192        192       6960          0          0 SCP Hybrid proce
  73  0          0          0      12960          0          0 ATM NP CLIENT PR
  74  0          0          0      12968          0          0 BRIDGING NP CLIE
  75  0          0          0       6960          0          0 fr_npc_dowork
  76  0        192        192       6968          0          0 fastblk backgrou
  77  0          0          0       6960          0          0 hnpc_dowork
  78  0          0          0      12968          0          0 SIP2 BRIDGE PROC
  79  0        192        192      12960          0          0 QoS NP Client
  80  0    2355016    1220392    2338776      12756          0 CEF LC IPC Backg
  81  0  112519984  111381200      72720          0          0 CEF LC Stats
  82  0          0          0       6960          0          0 CEF MQC IPC Back
  83  0          0          0       6960          0          0 TFIB LC cleanup
  84  0        192        192       6984          0          0 Any Transport ov
  85  0        192        192       6960          0          0 LOCAL AAA
  86  0        192        192       6960          0          0 AAA Cached Serve
  87  0        192        192       6960          0          0 RADIUS TEST CMD
  88  0        192        192       6960          0          0 AAA SEND STOP EV
  89  0        168          0       7128          0          0 CEF Scanner
  90  0          0          0       6968          0          0 SIP ATM cmd hand
  91  0          0          0       6968          0          0 SONET alarm time
  92  0          0          0       6960          0          0 Net Input
  93  0        192        192       6960          0          0 Compute load avg
  94  1      90632      89968      18392          0          0 console_rpc_serv
                                121804560 Total
------------------ show process cpu ------------------
CPU utilization for five seconds: 2%/0%; one minute: 2%; five minutes: 2%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           0         1          0  0.00%  0.00%  0.00%   0 Chunk Manager
   2           4     14151          0  0.00%  0.00%  0.00%   0 Load Meter
   3           0         1          0  0.00%  0.00%  0.00%   0 SCP async: CWAN-
   4        9816      7180       1367  0.16%  0.01%  0.00%   0 Check heaps
   5           0        23          0  0.00%  0.00%  0.00%   0 Pool Manager
   6           0         2          0  0.00%  0.00%  0.00%   0 Timers
   7           0         1          0  0.00%  0.00%  0.00%   0 AAA_SERVER_DEADT
   8           0         2          0  0.00%  0.00%  0.00%   0 AAA high-capacit
   9           0         2          0  0.00%  0.00%  0.00%   0 Serial Backgroun
  10         840     14179         59  0.00%  0.00%  0.00%   0 ENVM Background
  11           0      1180          0  0.00%  0.00%  0.00%   0 IPC Dynamic Cach
  12          72      1182         60  0.00%  0.00%  0.00%   0 PROCMIB LC Proce
  13           0         1          0  0.00%  0.00%  0.00%   0 IPC BackPressure
  14          36     70728          0  0.00%  0.00%  0.00%   0 IPC Periodic Tim
  15          44     70728          0  0.00%  0.00%  0.00%   0 IPC Deferred Por
  16          12        19        631  0.00%  0.00%  0.00%   0 IPC Seat Manager
  17           0         1          0  0.00%  0.00%  0.00%   0 SERIAL A'detect
  18        2956        38      77789  0.00%  0.00%  0.00%   0 SMART
  19           0         1          0  0.00%  0.00%  0.00%   0 Critical Bkgnd
  20          36     14355          2  0.00%  0.00%  0.00%   0 Net Background
  21           0        61          0  0.00%  0.00%  0.00%   0 Logger
  22         240     70728          3  0.00%  0.00%  0.00%   0 TTY Background
  23     1387988    138571      10016  2.04%  1.01%  1.04%   0 Per-Second Jobs
  24        4808      1218       3947  0.00%  0.01%  0.00%   0 Per-minute Jobs
  25           0         2          0  0.00%  0.00%  0.00%   0 SCP Multicast
  26           0         1          0  0.00%  0.00%  0.00%   0 Inode Table Dest
```

```
  27           0          3          0  0.00%  0.00%  0.00%   0 LC to RP  defere
  28           0         26          0  0.00%  0.00%  0.00%   0 CWLC IFCOM Proce
  29           0          1          0  0.00%  0.00%  0.00%   0 IPC RTTYC Messag
  30           0          2          0  0.00%  0.00%  0.00%   0 INTR MGR PROCESS
  31           0         11          0  0.00%  0.00%  0.00%   0 ixp_exmem_reuse_
  32           4         62         64  0.00%  0.00%  0.00%   0 spnpc_dowork
  33           0          1          0  0.00%  0.00%  0.00%   0 Spi4 Timer
  34           0          1          0  0.00%  0.00%  0.00%   0 LC interrupt, J1
  35           0          1          0  0.00%  0.00%  0.00%   0 SIP interrupt, P
  36           0          1          0  0.00%  0.00%  0.00%   0 SDCC Input
  37           0          2          0  0.00%  0.00%  0.00%   0 SDCC Periodic
  38           0          2          0  0.00%  0.00%  0.00%   0 SDCC IO
  39           0          1          0  0.00%  0.00%  0.00%   0 CWAN LTL manager
  40        1208      14154         85  0.00%  0.00%  0.00%   0 msg_handler_proc
  41         148      70730          2  0.00%  0.00%  0.00%   0 Cardmgr Periodic
  42           0          6          0  0.00%  0.00%  0.00%   0 SIP SWBus Sync P
  43           0          5          0  0.00%  0.00%  0.00%   0 NP doorbell proc
  44           0          5          0  0.00%  0.00%  0.00%   0 CardMgr Events
  45        1400         26      53846  0.00%  0.00%  0.00%   0 INP Reload
  46           0        379          0  0.00%  0.00%  0.00%   0 ipc_handler_proc
  47           0          5          0  0.00%  0.00%  0.00%   0 NP doorbell proc
  48        2224         25      88960  0.00%  0.00%  0.00%   0 ENP Reload
  49          16       1200         13  0.00%  0.00%  0.00%   0 ipc_handler_proc
  50           0          1          0  0.00%  0.00%  0.00%   0 SIP2 Bus Stall
  51      214912      53129       4045  0.00%  0.00%  0.00%   0 ifnpc_dowork
  52           0          4          0  0.00%  0.00%  0.00%   0 hmi_dowork
  53           0         31          0  0.00%  0.00%  0.00%   0 cwanlc_npc_dowor
  54           0          1          0  0.00%  0.00%  0.00%   0 VIP Encap IPC Ba
  55       18532     487255         38  0.00%  0.00%  0.00%   0 SPA OIR 5/0
  56          84       2372         35  0.00%  0.00%  0.00%   0 SPA OIR 5/1
  57          80       2368         33  0.00%  0.00%  0.00%   0 SPA OIR 5/2
  58          84       2368         35  0.00%  0.00%  0.00%   0 SPA OIR 5/3
  59        2432         32      76000  0.00%  0.00%  0.00%   0 LC FPD Upgrade P
  60        3112     138447         22  0.00%  0.00%  0.00%   0 spa_env_monitor
  61           0          2          0  0.00%  0.00%  0.00%   0 AAA Dictionary R
  62           0          2          0  0.00%  0.00%  0.00%   0 AAA Server
  63           0          1          0  0.00%  0.00%  0.00%   0 AAA ACCT Proc
  64           0          1          0  0.00%  0.00%  0.00%   0 ACCT Periodic Pr
  65           0          2          0  0.00%  0.00%  0.00%   0 ATMLS task
  66           0       7185          0  0.00%  0.00%  0.00%   0 AToM NP CLIENT B
  67          16       7185          2  0.00%  0.00%  0.00%   0 TTFIB NP CLIENT
  68           8     707134          0  0.00%  0.00%  0.00%   0 SSA FABLINK Proc
  69           0      14150          0  0.00%  0.00%  0.00%   0 HYP ACCU FAB COU
  70        7140     103916         68  0.00%  0.00%  0.00%   0 CEF process
  71           0          2          0  0.00%  0.00%  0.00%   0 CWTLC SSO Proces
  72         328       4423         74  0.00%  0.00%  0.00%   0 SCP Hybrid proce
  73           4      77777          0  0.00%  0.00%  0.00%   0 ATM NP CLIENT PR
  74         324      70733          4  0.00%  0.00%  0.00%   0 BRIDGING NP CLIE
  75          12       7182          1  0.00%  0.00%  0.00%   0 fr_npc_dowork
  76           4     707140          0  0.00%  0.00%  0.00%   0 fastblk backgrou
  77          40          2      20000  0.00%  0.00%  0.00%   0 hnpc_dowork
  78           0          1          0  0.00%  0.00%  0.00%   0 SIP2 BRIDGE PROC
  79         416       7079         58  0.00%  0.00%  0.00%   0 QoS NP Client
  80        3300     726380          4  0.00%  0.00%  0.00%   0 CEF LC IPC Backg
  81         628      93426          6  0.00%  0.00%  0.00%   0 CEF LC Stats
  82           0          1          0  0.00%  0.00%  0.00%   0 CEF MQC IPC Back
  83           0          1          0  0.00%  0.00%  0.00%   0 TFIB LC cleanup
  84           0          2          0  0.00%  0.00%  0.00%   0 Any Transport ov
  85           0          2          0  0.00%  0.00%  0.00%   0 LOCAL AAA
  86           0          2          0  0.00%  0.00%  0.00%   0 AAA Cached Serve
  87           0          3          0  0.00%  0.00%  0.00%   0 RADIUS TEST CMD
  88           0          2          0  0.00%  0.00%  0.00%   0 AAA SEND STOP EV
  89         128       5003         25  0.00%  0.00%  0.00%   0 CEF Scanner
  90           0          1          0  0.00%  0.00%  0.00%   0 SIP ATM cmd hand
```

```
  91           0         1          0  0.00%  0.00%  0.00%   0 SONET alarm time
  92           0         1          0  0.00%  0.00%  0.00%   0 Net Input
  93          16     14775          1  0.00%  0.00%  0.00%   0 Compute load avg
  94          92       502        183  0.00%  0.09%  0.02%   1 console_rpc_serv
------------------ show process cpu history ------------------


     22222222223333322222222222222222222221111122222222222222222222
100
 90
 80
 70
 60
 50
 40
 30
 20
 10
    0....5....1....1....2....2....3....3....4....4....5....5....
              0    5    0    5    0    5    0    5    0    5
               CPU% per second (last 60 seconds)

                1           1 1  1
     222222222223322222222222424324322222222222222222222222222222
100
 90
 80
 70
 60
 50
 40
 30
 20
 10             *           * *  *
    0....5....1....1....2....2....3....3....4....4....5....5....
              0    5    0    5    0    5    0    5    0    5
               CPU% per minute (last 60 minutes)
              * = maximum CPU%   # = average CPU%

     1                 9
     4222222222222222229
100                    *
 90                    *
 80                    *
 70                    *
 60                    *
 50                    *
 40                    *
 30                    *
 20                    *
 10  *                 *
    0....5....1....1....2....2....3....3....4....4....5....5....6....6....7.
              0    5    0    5    0    5    0    5    0    5    0    5    0
                   CPU% per hour (last 72 hours)
                  * = maximum CPU%   # = average CPU%
------------------ show file systems ------------------
File Systems:
     Size(b)     Free(b)      Type  Flags  Prefixes
           -           -    opaque     rw   system:
           -           -    opaque     rw   null:
           -           -    opaque     ro   tar:
*   64097280    40606720      disk     rw   disk0:
------------------ show disk0: all ------------------
-#- --length-- -----date/time------ path
```

```
 number of file 8
 inode path is 1 idprom-oc12-atm-superspa
 fullpath is disk0:/idprom-oc12-atm-superspa
1         1152 Jun 09 2004 13:03:38 idprom-oc12-atm-superspa
 inode path is 2 idprom-4oc3-atm-superspa
 fullpath is disk0:/idprom-4oc3-atm-superspa
2         1152 Jun 09 2004 05:51:34 idprom-4oc3-atm-superspa
 inode path is 3 bonham_brd_rev2_rev19.hex
 fullpath is disk0:/bonham_brd_rev2_rev19.hex
3      2626407 Aug 24 2004 11:04:42 bonham_brd_rev2_rev19.hex
 inode path is 4 sip2-dw-mz.b2-testt
 fullpath is disk0:/sip2-dw-mz.b2-testt
4      5895640 Aug 26 2004 05:09:08 sip2-dw-mz.b2-testt
 inode path is 5 sip2-dw-mz.hp-depth
 fullpath is disk0:/sip2-dw-mz.hp-depth
5      5897476 Aug 12 2004 04:40:38 sip2-dw-mz.hp-depth
 inode path is 6 viking1.jbc
 fullpath is disk0:/viking1.jbc
6      2678150 Jun 09 2004 12:48:32 viking1.jbc
 inode path is 7 sip2-dw-mz.hpd
 fullpath is disk0:/sip2-dw-mz.hpd
7      5916716 Aug 25 2004 10:25:14 sip2-dw-mz.hpd
 inode path is 8 sip2iofpga_promlatest_rev78.hex
 fullpath is disk0:/sip2iofpga_promlatest_rev78.hex
8       468975 Aug 24 2004 10:56:54 sip2iofpga_promlatest_rev78.hex
40606720 bytes available (23490560 bytes used)
******** ATA Flash Card Geometry/Format Info ********
ATA CARD GEOMETRY
   Number of Heads:       4
   Number of Cylinders    984
   Sectors per Cylinder   32
   Sector Size            512
   Total Sectors          125952
ATA CARD FORMAT
   Number of FAT Sectors  246
   Sectors Per Cluster    2
   Number of Clusters     62595
   Number of Data Sectors 125817
   Base Root Sector       595
   Base FAT Sector        103
   Base Data Sector       627
------------------ show scp status ------------------
Rx 29169,  Tx 29165,  Sap 3  scp_my_addr 0x4
Id Sap      Channel name    current/peak/retry/dropped/total  time(queue/process/ack)
-- ---- ------------------- --------------------------------  ----------------------
0  0    SCP Unsolicited:0       0/    2/    0/      0/ 4421       0/    0/  76
1  23   SCP async: CWAN-NMP     0/    0/    0/      0/    0       0/    0/   0
------------------ show inventory ------------------
------------------ show region ------------------
Region Manager:
      Start         End     Size(b)  Class  Media  Name
 0x0F000000  0x0FFFFDFF    16776704  Iomem  R/W    iomem
 0x40000000  0x4EFFFFFF   251658240  Local  R/W    main
 0x40010FC0  0x4067FFE7     6746152  IText  R/O    main:text
 0x40680000  0x40CE977F     6723456  IData  R/W    main:data
 0x40CE9780  0x4145B85F     7807200  IBss   R/W    main:bss
 0x4145B860  0x4EFFFFFF   230311840  Local  R/W    main:heap
 0x80000000  0x8EFFFFFF   251658240  Local  R/W    main:(main_k0)
 0xA0000000  0xAEFFFFFF   251658240  Local  R/W    main:(main_k1)
------------------ show buffers ------------------
Buffer elements:
     500 in free list (500 max allowed)
     595460 hits, 0 misses, 0 created
Public buffer pools:
```

```
Small buffers, 104 bytes (total 37, permanent 25, peak 39 @ 19:39:17):
     35 in free list (20 min, 60 max allowed)
     310581 hits, 48 misses, 110 trims, 122 created
     0 failures (0 no memory)
Middle buffers, 600 bytes (total 15, permanent 15, peak 21 @ 19:39:19):
     14 in free list (10 min, 30 max allowed)
     20386 hits, 2 misses, 6 trims, 6 created
     0 failures (0 no memory)
Big buffers, 1536 bytes (total 6, permanent 5, peak 8 @ 19:39:21):
     6 in free list (5 min, 10 max allowed)
     16375 hits, 1 misses, 11 trims, 12 created
     0 failures (0 no memory)
VeryBig buffers, 4520 bytes (total 50, permanent 50):
     50 in free list (40 min, 300 max allowed)
     0 hits, 0 misses, 0 trims, 0 created
     0 failures (0 no memory)
Large buffers, 5024 bytes (total 0, permanent 0):
     0 in free list (0 min, 5 max allowed)
     0 hits, 0 misses, 0 trims, 0 created
     0 failures (0 no memory)
Huge buffers, 18024 bytes (total 1, permanent 1):
     1 in free list (0 min, 2 max allowed)
     0 hits, 0 misses, 0 trims, 0 created
     0 failures (0 no memory)
Interface buffer pools:
IPC buffers, 4096 bytes (total 85, permanent 16, peak 85 @ 00:00:36):
     12 in free list (10 min, 30 max allowed)
     251678 hits, 23 fallbacks, 0 trims, 69 created
     0 failures (0 no memory)
Header pools:
SDCC Packet Header buffers, 0 bytes (total 2048, permanent 2048):
     0 in free list (2048 min, 2048 max allowed)
     2048 hits, 0 misses
     2048 max cache size, 2048 in cache
     0 hits in cache, 0 misses in cache
Particle Clones:
     2048 clones, 0 hits, 0 misses
Public particle pools:
GLOBAL buffers, 512 bytes (total 862, permanent 862):
     0 in free list (0 min, 862 max allowed)
     862 hits, 0 misses
     862 max cache size, 862 in cache
     0 hits in cache, 0 misses in cache
COMM buffers, 512 bytes (total 32, permanent 32):
     0 in free list (0 min, 32 max allowed)
     32 hits, 0 misses
     32 max cache size, 32 in cache
     0 hits in cache, 0 misses in cache
Private particle pools:
SB-FIFO5/0/1 buffers, 512 bytes (total 1000, permanent 1000):
     0 in free list (0 min, 1000 max allowed)
     1000 hits, 0 fallbacks
     1000 max cache size, 744 in cache
     261 hits in cache, 0 misses in cache
     14 buffer threshold, 0 threshold transitions
EOBC0/0 buffers, 512 bytes (total 2000, permanent 2000):
     0 in free list (0 min, 2000 max allowed)
     2000 hits, 0 misses
     2000 max cache size, 1744 in cache
     79803 hits in cache, 0 misses in cache
     14 buffer threshold, 0 threshold transitions
Ingress ESF Engine buffers, 1028 bytes (total 21, permanent 21):
     0 in free list (21 min, 21 max allowed)
     21 hits, 0 misses
```

```
     21 max cache size, 0 in cache
     21 hits in cache, 0 misses in cache
Egress ESF Engine buffers, 1028 bytes (total 21, permanent 21):
     0 in free list (21 min, 21 max allowed)
     21 hits, 0 misses
     21 max cache size, 0 in cache
     21 hits in cache, 0 misses in cache
------------------ show platform hardware version ------------------
        Product Number: '7600-MSC-400'
        Baseboard Serial Number: 'SAD073101T6'
        Manufacturing Assembly Revision: 'A01'
        Baseboard Revision: 0.14
        Daughtercard Serial Number: ''
        CPU Manufacturer: 0x4 (Broadcom)
        CPU SOC Type: BCM1125H 400 Mhz rev 0x21 wafer 0x1
        CPU Revision: 0.3
        Super Santa Ana: 0x0
        PM PLD: 0x5
        IOFPGA version: 0x00051
               type:    0x0 format 0x2 loaded from Upgrade (C1) region
        ROMMON (major.minor.dev.build) = 1.1.0.1
        Bonham version: 0x019
               type:    rev2-or-higher-bb
        Gldfgr version: 0x10014
        Oddjob version: 0x10010
        Hyperion: 0x2
        Config PLD: 0x6
        Ingress ESF Engine          : Type 0.0 rev 0.2, 1400 MHz
                                      SRAM clocks: 140/200/200/200 MHz
                                      DRAM clock: 400 MHz
        Egress ESF Engine           : Type 0.0 rev 0.2, 1400 MHz
                                      SRAM clocks: 200/200/140/200 MHz
                                      DRAM clock: 400 MHz
------------------ show platform hardware iofpga ------------------
CPU base address:       0xB1000000
0000: type_and_version: 0x00000251
0004: global_intr_en:   0x100D1021
0008: global_intr_stat: 0x00000008
000C: reset_reason_reg: 0x00000001
0010: cpu_resets:       0x00000000
0014: device_reset:     0x00000040
0018: watchdog:         0x00003D96
001C: who_am_i:         0x00002200
0020: rommon_sel:       0x00000001
0024: led_reg:          0x0000001F
0028: iofpga_ctrl:      0x00000400
002C: earl_control:     0x0000000F
0030: iobus_intr_en:    0x0000000F
0034: iobus_intr_stat:  0x00000000
0038: iobus_deadman:    0x00000015
003C: iobus_last_addr:  0x00000000
0040: iobus_last_data:  0x00000000
0044: iobus_tran_stat:  0x00000000
0048: test_pins_reg:    0x00000000
0058: pld_jtag:         0xCAFEBABE
SIP2 base addr:   0xB1000400
0000: spa_ctrl:         0x00000923
0004: spa_intr_en:      0x7E07222F
0008: spa_intr_stat:    0x01000000
000C: spa_stat:         0x0000222C
0010: spabus_deadman:   0x0000002A
0014: spabus_tran_stat: 0x0800021C
0018: spabus_last_read: 0x00070001
001C: spabus_last_par:  0x00003531
```

```
0020: spa_test:         0xAB2B2B29
0024: spd_ctrl:         0x00000007
0028: scratchpad:       0x00000000
002C: ha_state:         0x00000001
0030: spa0_debounce:    0x0000000A
0034: spa1_debounce:    0x0000000A
0038: spa2_debounce:    0x0000000A
003C: spa3_debounce:    0x0000000A
0044: ha_sanity:        0x00000007
0040: spa_sonet_clk:    0x200AD500
0048: spa_sonet_clk_ie: 0x00000000
004C: spa_sonet_clk_is: 0x1FFFFFFC
0050: spa_sonet_clk_div[0]: 0x0000097E
0054: spa_sonet_clk_div[1]: 0x0000097E
0058: spa_sonet_clk_div[2]: 0x0000097E
005C: spa_sonet_clk_div[3]: 0x0000097E
```

show hw-module subslot

To display diagnostic information about internal hardware devices for a SPA, use the **show hw-module subslot** command in privileged EXEC configuration mode.

To display diagnostic information about modules and interfaces on a Cisco 4400 Series ISR, use the **show hw-module subslot** command in privileged EXEC mode.

show hw-module subslot [*slot*/*subslot*] {**brief** | **config** | **counters** | **errors** | **registers** | **status**} **device** *port*

Cisco 4400 Series Integrated Services Router (ISR)

show hw-module subslot [*slot*/*subslot*]
all | **attribute** | **entity** | **fpd** | **oir** | **sensors** | **subblock**

Syntax Description

slot	(Optional) Chassis slot number or module interface slot number. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide. For more information on slots for the Cisco 4400 Series ISR, refer to hardware installation guide.
/subslot	(Optional) Secondary slot number on a SIP where a SPA is installed. Refer to the platform-specific SPA hardware installation guide and the corresponding "Specifying the Interface Address on a SPA" topic in the platform-specific SPA software configuration guide for subslot information. For more information on subslots for the Cisco 4400 Series ISR, refer to hardware installation guide.
all*subslot*	Selects all supported modules and displays diagnostic and register information related to the modules including: • **attribute**--Detailed module attribute information • **entity**--MIB details of an entity[1]. • **fpd**--Field programmable devices (fpd) information • **oir**--Online insertion and removal (oir) summary • **sensors**--Environmental sensor summary • **subblock**--Internal data structure related to the supported module[1] • **tech-support**--Subslot information for technical support

brief config | **counters errors** | **registers status**	Specifies the display of diagnostic and register information related to the following areas: • **brief**--Reserved for future. • **config**--Displays information related to configuration of the specified internal hardware device. • **counters**--Displays statistics related to the processing by the specified internal hardware device. • **errors**--Reserved for future. • **registers**--Displays register information for the specified internal hardware device. • **status**--Displays status information for the specified internal hardware device.
device	Specifies the internal hardware device or path on the SPA for which you want to display diagnostic information, including the field programmable gate array (FPGA) device, MAC device, PHY device, or System Packet Interface Level 4 (SPI4) path from the MSC to the FPGA device.
port	(Optional) Port or interface number. Refer to the appropriate hardware manual for port information. For SPAs, refer to the corresponding "Specifying the Interface Address on a SPA" topics in the platform-specific SPA software configuration guide.

Command Default

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(20)S2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.9S	This command was implemented on Cisco 4400 Series ISR and integrated into Cisco IOS XE Release 3.9 S.

Usage Guidelines

Use the **show hw-module subslot** command to obtain diagnostic information about an interface on the SPA.

The **counters** keyword displays a subset of the statistics that are also provided by the **show controllers fastethernet** command for the specified SPA device.

Use the **show hw-module subslot** command in Cisco 4400 Series ISRs to obtain diagnostic information related to all supported Cisco services modules and network interface modules(NIM). You can use the **show hw-module subslot all oir** command to verify the operation and proper activation of a module after an online insertion or removal.

Show hw-module subslot all oir Example

The following sample output from the **show hw-module subslot all oir** command verifies activation and proper operation of all supported modules on the router:

```
Router#show hw-module subslot all oir

 Module          Model               Operational Status

-------------- ------------------ -------------------------

subslot 0/1    NIM-8MFT-T1/E1       ok
subslot 1/0    SM-X T1/E1           ok
```

Examples

The following examples provide sample output for several versions of the **show hw-module subslot** command for a SPA located in the top subslot (0) of the MSC that is installed in slot 4 on a Cisco 7304 router.

show hw-module subslot config fpga Example

The following shows sample output from the **show hw-module subslot config** command for the FPGA device on the first interface (port 0):

```
Router# show hw-module subslot 4/0 config fpga 0
FPGA RX Config
  RX FIFO parity select is even
  RX CRC check is  enabled
  RX SHIM header insertion is  disabled
  RX Flow control is enabled
  RX CRC strip is  enabled
  RX TCAM LKUP is enabled
FPGA TX Config
  TX FIFO parity select is even
  TX CRC generation is enabled
  TX Padding is enabled
```

show hw-module subslot config phy Example

The following shows sample output from the **show hw-module subslot config** command for the PHY device on the first interface (port 0):

```
Router# show hw-module subslot 4/0 config phy 0
  PHY version: identifier1 = 0x141, identifier2 = 0xCD2
  PHY Configuration:
  control (reg 0) = 0x3100
    PHY state: not in reset, not powered down, not isoloated
    speed: 100 Mbps, duplex: full
    auto-negotiation enabled, loopback disabled, collision test disabled
  phy specific control (reg 16) = 0x78
    force link good: no
    MDI cross-over mode: automatic crossover
    Tx FIFO depth: +/- 16 bits, Rx FIFO depth: +/- 16 bits
    never assert CRS on transmit, energy detect: off
```

```
    enable extended distance: no, 125 clock: low
    MAC interface power: always up, SQE test: disabled
    polarity reversal: enabled, jabber function: enabled
  extended phy specific control (reg 20) = 0xCE2
    line loopback: disabled, detect lost lock: no, enabled RCLK
    master downshift counter: 4, slave downshift counter: 0
    default MAC interface speed: 1000 Mbps
    fiber auto-negotiation disabled
    add delay to RX_CLK for RXD outputs: yes
    add delay to GTX_CLK for TXD latching: yes
  auto-negotiation advertisement for 10/100 (reg 4) = 0xDE1
    10Base-Tx half-duplex: yes, full-duplex: yes
    100Base-Tx half-duplex: yes, full-duplex: yes
    pause frame support: yes, asymmetric pause: yes
    set remote fault bit: no, advertise next page: no
```

show hw-module subslot counters fpga Example

The following shows sample output from the **show hw-module subslot counters** command for the FPGA device on the first interface (port 0):

Note This information is also available using the **show controllers fastethernet** command.

```
Router# show hw-module subslot 4/0 counters fpga 0
Input: Total (good & bad) packets: 5734
         TCAM drops: 4908
         Satisfy (host-backpressure) drops: 0
         CRC drops: 0
         PL3 RERRs: 0
  Output: EOP (SPI4) errors: 0
```

show hw-module subslot status mac Example

The following shows sample output from the **show hw-module subslot** command for MAC device status on the first interface (port 0):

```
Router# show hw-module subslot 4/0 status mac 0
  Status registers:
    speed = 100 Mbps, duplex = full, interface mode = copper
    spi3 side loopback is disabled, line side loopback is disabled
    padding is disabled, crc add is disabled
    force duplex is enabled
  Rx FIFO status:
    Read pointer = 0xCDE, Write pointer = 0xCDE
    Occupancy of FIFO in 8 byte locations = 0
    Reset is not set
    Overflow event did not occur
  Tx FIFO status:
    Read pointer = 0x498, Write pointer = 0x498
    Occupancy of FIFO in 8 byte locations = 0
    Overflow event did not occur
    Underflow event did not occur
    Out of sequence event did not occur
```

show hw-module subslot status phy Example

The following shows sample output from the **show hw-module subslot** command for PHY device status on the first interface (port 0):

```
Router# show hw-module subslot 4/0 status phy 0
  PHY Status:
  status (reg 1) = 0x7949
    link is down, auto-negotiation is not complete
    remote fault not detected, jabber not detected
  phy specific status (reg 17) = 0x4100
    link is down (real-time), speed/duplex not resolved
    speed: 100 Mbps, duplex: half
    page not received, cable length is 80 - 110m
    MDI cross-over status: MDI, downshift status: no
    energy detect status: active
    transmit pause: disabled, receive pause: disabled
    polarity: normal, jabber: no
  phy specific extended status (reg 27) = 0x848B
    Fiber/ copper auto selection disabled, copper link
    Serial interface auto-negotiation bypass disabled
    Serial interface auto-negotiation bypass status:
      Link came up because regular fiber autoneg completed
    Interrupt polarity is active low
  receive error count: 0x0
```

Related Commands

Command	Description
hw-module subslot service-engine session	Opens a session on the Cisco WebEx Node SPA console.
service-engine default-gateway	Defines a default gateway router IP address for the Cisco WebEx Node SPA.
service-engine ip address	Selects and configures the internal interface for management traffic on a Cisco WebEx Node SPA.
service-engine hostname	Specifies or modifies the hostname or domain name associated with a Cisco WebEx Node SPA.
service-engine nameserver	Specifies the primary and secondary domain name server used by the Cisco WebEx Node SPA.
service-engine wma-passcode	Configures the name and that are used for authentication on a Cisco WebEx Node SPA.
service-engine wma-token	Configures an encrypted token on a Cisco WebEx Node SPA.
service-engine wma-url	Specifies the URL to which the Cisco WebEx Node SPA must connect to enable WebEx meetings.

show hw-module subslot fpd

To display the current versions of all field-programmable devices (FPDs) for a particular SPA or all of the active SPAs on a router, use the **showhw-modulesubslotfpd** command in privileged EXEC mode.

Cisco 7304 Router
show hw-module subslot [*slot*/*subslot*] **fpd**

Cisco 7600 Series Routers, Catalyst 6500 Series Switches, Cisco 12000 Series Routers, and Cisco uBR10012 Universal Broadband Router
show hw-module subslot {*slot*/*subslot* | **all**} **fpd**

Syntax Description

slot	Chassis slot number. Refer to the platform-specific SPA hardware installation guide and the corresponding “Identifying Slots and Subslots for SIPs and SPAs” topic in the platform-specific SPA software configuration guide.
subslot	Secondary slot number on a SPA interface processor (SIP) where a SPA is installed. Refer to the platform-specific SPA hardware installation guide and the corresponding “Specifying the Interface Address on a SPA” topic in the platform-specific SPA software configuration guide for subslot information.
all	Specifies display of FPD information for all SPAs in the system. **Note** The **all** keyword is not supported for SPAs on the Cisco 7304 router.

Command Default

For the Cisco 7304 router, if no location is specified, the output for this command will show information for all supported card types on the router.

For the Cisco 7600 series routers, Catalyst 6500 series switches, and Cisco 12000 series routers, there is no default behavior or values.

For more information about FPD upgrades on shared port adapters (SPAs), refer to the Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(20)S2	This command was introduced.
12.2(18)SXE	The **all** keyword was added in Cisco IOS Release 12.2(18)SXE on the Cisco 7600 series routers and Catalyst 6500 series switches.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S and introduced on Cisco 12000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.

Usage Guidelines

Other than the FPD version information, the output for this command may also contain useful FPD-related notes.

Cisco 7304 Router

The **all** keyword is not supported on the Cisco 7304 router. The *slot/subslot* arguments are optional, and if you do not specify them, the command displays FPD information for all supported card types on the router.

Cisco 7600 Series Routers, Catalyst 6500 Series Switches, 12000 Series Routers, and Cisco uBR10012 Universal Broadband Router

If you do not use the **all** keyword, then you must specify the *slot/subslot* arguments to select the location of a particular card. There is no default behavior for this command on the Cisco 7600 series routers.

Examples

Displaying FPD Information for a Particular SPA Example

This example shows the output when using the *slot/subslot* arguments to identify a particular SPA. This SPA meets the minimum FPD requirements with that particular Cisco IOS release.

```
Router#
show hw-module subslot 4/0 fpd
==== ====================== ====== =============================================
                             H/W   Field Programmable   Current   Min. Required
Slot Card Description        Ver.  Device: "ID-Name"    Version      Version
==== ====================== ====== ================== =========== ==============
4/0 SPA-4XOC3-ATM           1.0   1-I/O FPGA            0.121       0.121
==== ====================== ====== =============================================
```

Cisco uBR10012 Universal Broadband Router

The following example shows the output when using the *slot/subslot* arguments to identify a particular SPA on a Cisco uBR10012 router:

```
Router#
show hw-module subslot 3/1 fpd
==== ====================== ====== =============================================
                             H/W   Field Programmable   Current   Min. Required
Slot Card Type               Ver.  Device: "ID-Name"    Version      Version
==== ====================== ====== ================== =========== ==============
3/1 SPA-24XDS-SFP           1.0   1-Modena BLAZE FPG  1285.1444   1285.1444
==== ====================== ====== =============================================
```

Displaying FPD Information for all SPAs in the System Example

This example shows FPD image file versions for all SPAs in the system:

```
Router# show hw-module subslot all fpd
==== ====================== ====== =============================================
                             H/W   Field Programmable   Current   Min. Required
Slot Card Type               Ver.  Device: "ID-Name"    Version      Version
==== ====================== ====== ================== =========== ==============
 4/0 SPA-4XOC3-ATM           1.0   1-I/O FPGA             0.121       0.121
---- ---------------------- ------ ------------------ ----------- --------------
 4/1 SPA-8XT1/E1             0.143 1-ROMMON               2.12        2.12
```

```
                              2-I/O FPGA            0.22        0.22
---- ---------------------- ------ ------------------ ----------- --------------
 4/3 SPA-4XOC3-POS          0.100 1-I/O FPGA            3.4         3.4
---- ---------------------- ------ ------------------ ----------- --------------
 7/0 SPA-8XCHT1/E1          0.117 1-ROMMON              2.12        2.12
                                  2-I/O FPGA            0.22        0.22
---- ---------------------- ------ ------------------ ----------- --------------
 7/1 SPA-4XOC3-ATM          0.205 1-I/O FPGA            0.121       0.121
==== ====================== ====== =============================================
```

Cisco uBR10012 Universal Broadband Router

The following example shows FPD image file versions for all SPAs on a Cisco uBR10012 router:

```
Router#
show hw-module subslot all fpd
==== ====================== ====== =============================================
                            H/W    Field Programmable   Current   Min. Required
Slot Card Type              Ver.   Device: "ID-Name"    Version      Version
==== ====================== ====== ================== =========== ==============
 3/0 SPA-24XDS-SFP          1.0    1-Modena BLAZE FPG  1285.1444   1285.1444
---- ---------------------- ------ ------------------ ----------- --------------
 3/1 SPA-24XDS-SFP          1.0    1-Modena BLAZE FPG  1285.1444   1285.1444
---- ---------------------- ------ ------------------ ----------- --------------
 3/2 SPA-1X10GE-L-V2        1.2    1-10GE V2 I/O FPGA     1.9         1.9
---- ---------------------- ------ ------------------ ----------- --------------
 3/3 SPA-5X1GE-V2           1.2    1-5xGE V2 I/O FPGA     1.10        1.10
==== ====================== ====== =============================================
```

Displaying Information for all SPAs in the System Example (Cisco 7304 only)

The **all** keyword is not supported on the Cisco 7304 router.

To display all FPD image file versions for all SPAs on a Cisco 7304 router, enter the **showhw-modulesubslotfpd** command without specifying a slot and subslot. The following example shows all FPD image file versions on a Cisco 7304 router:

```
Router# show hw-module subslot fpd
==== ====================== ====== =============================================
                            H/W    Field Programmable   Current   Min. Required
Slot Card Description       Ver.   Device:"ID-Name"     Version      Version
==== ====================== ====== ================== =========== ==============
 2/0 SPA-4FE-7304           0.32
1-Data & I/O FPG
A      4.13         4.13
---- ---------------------- ------ ------------------ ----------- --------------
 2/1 SPA-2GE-7304           0.15
1-Data & I/O FPG
A      4.13         4.13

==== ====================== ======
=============================================
```

Related Commands

Command	Description
show hw-module all fpd	Displays the current versions of all FPDs for all of the supported card types on a router.
show hw-module slot fpd	Displays the current versions of all FPDs for a SIP in the specified slot location on a router, and for all of the SPAs installed in that SIP.

show hw-module subslot oir

To display the operational status of a shared port adapter (SPA), use the **showhw-modulesubslotoir** command in privileged EXEC configuration mode.

show hw-module subslot {*slot* / *subslot* | **all**} **oir** [**internal**]

Syntax Description

slot	Chassis slot number. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding “Identifying Slots and Subslots for SIPs and SPAs” topic in the platform-specific SPA software configuration guide.
/ *subslot*	Secondary slot number on a SPA interface processor (SIP) where a SPA is installed. Refer to the platform-specific SPA hardware installation guide and the corresponding “Specifying the Interface Address on a SPA” topic in the platform-specific SPA software configuration guide for subslot information.
all	Displays OIR status for all supported card types in the system.
internal	(Optional) Displays detailed diagnostic information. This option is intended for internal diagnostic use with Cisco Systems technical support personnel.

Command Default

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)S3	This command was introduced.
12.2(18)SXE	Thiscommand was integrated into Cisco IOS Release 12.2(18)SXE.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **showhw-modulesubslotoir** command to obtain operational status information about one or all SPAs. To display information for a specific SPA, specify the slot number of the SIP and the subslot number of the SPA about which you want information.

To display information for all SPAs in the router, do not specify the *slot*/*subslot* arguments and use the **all** keyword. If no location is specified, the output for this command will show information for all SPAs in the router.

The optional **internal** keyword displays detailed diagnostic information that is recommended only for use with Cisco Systems technical support personnel.

Examples

The following example shows the operational status of all of the SPAs installed in a router where two of the SPAs are in an out-of-service condition:

```
Router# show hw-module subslot all oir
Module         Model              Operational Status
-------------- ------------------ -------------------------
subslot 4/0    SPA-4XOC3-POS      booting
subslot 4/1    SPA-4XOC3-ATM      out of service(FPD upgrade failed)
subslot 4/2    SPA-4XOC3-POS      ok
subslot 4/3    SPA-1XTENGE-XFP    out of service(SPA unrecognized)
```

The table below describes the possible values for the Operational Status field in the output.

Note The following status descriptions are not applicable to every SPA and can be platform-specific.

Table 111: Operational Status Field Descriptions

Operational Status	Description
admin down	SPA is administratively disabled by the **hw-modulesubslotshutdown** global configuration command.
booting	SPA is initializing.
missing	SPA is not present in the SIP subslot.
ok	SPA is operational.
out of service (*reason*)	The SPA is out of service for one of the following reasons: **Note** The following reasons are not applicable to every SPA and can be platform-specific. • Analyze failed--Failed to create a SPA data structure, most likely due to a memory allocation problem. • Authentication failed--A SPA has failed hardware validation. • Data structure create error--Failed to create a SPA data structure, most likely due to a memory allocation problem. • Event corrupt--A SPA online insertion and removal (OIR) event has been corrupted. This could be caused by a corrupted message between the SIP and the Route Processor (RP) or some other software or hardware problem. • Event sequence error--A SPA OIR event was received out of sequence. This could be caused by a corrupted message between the SIP and the Route Processor (RP) or some other software or hardware problem. • Fail code not set--Failure code could not be read from a SPA OIR event message. This could be caused by a corrupted message between the SIP and the RP or some other software or hardware problem. • Failed too many times--A SPA is disabled because it has failed more than the allowable limit on the platform.

Operational Status	Description
	• FPD upgrade failed--A field-programmable device, such as the Field-Programmable Gate Array (FPGA), failed to automatically upgrade. • H/W signal deasserted--The SPA_OK or PWR_OK hardware signal indicating that the SPA is accessible is no longer asserted. • Heartbeat failed--Occurs when intelligent SPAs encounter heartbeat failures. • Incompatible FPD--An FPGA version mismatch with the Cisco IOS software has been detected for the SPA. • Init timeout--Time limit has been reached during initialization of a SPA. • Read SPA type failed--A read from the hardware for the SPA type failed. • Reload request--A SPA reload is in progress from the **hw-modulesubslotreload** command. • SPA h/w error--The SPA software driver has detected a hardware error. • SPA ready timeout--A timeout ocurred on the RP while waiting for the SPA to become operational. • SPA type mismatch--Occurs when you have preconfigured a SPA of one type, but have inserted a SPA of a different type. **Note** This reason code only applies to those platforms that support pre-configuration. This is not applicable to a Cisco 7600 series router or Catalyst 6500 series switch. • SPA unrecognized--SPA is not supported by the Cisco IOS software release. • Start failed--Failed to start interfaces on SPA. • Unexpected inserted event--The SPA OIR software has received a SPA insertion event when the OIR software considered the SPA already present. • Wait h/w ok timeout--A timeout occurred while waiting for the SPA_OK and PWR_OK hardware signals to be asserted. • Wait start timeout--A timeout occurred on the SIP while waiting for permission from the RP to bring up the SPA.
stopped	SPA has been gracefully deactivated using the **hw-modulesubslotstop** privileged EXEC command on the Cisco 7304 router.

The following example shows the operational status of all of the SPAs installed in a router where all SPAs are running successfully:

```
Router# show hw-module subslot all oir

Module        Model                Operational Status
------------- -------------------- ------------------------
```

```
subslot 1/1   SPA-2XOC3-ATM        ok
subslot 4/0   SPA-2XT3/E3          ok
subslot 4/1   SPA-4XOC3-POS        ok
subslot 4/2   SPA-8XCHT1/E1        ok
```

The following example shows sample output when using the optional **internal** keyword:

```
Router# show hw-module subslot 4/0 oir internal
WARNING: This command is not intended for production use
and should only be used under the supervision of
Cisco Systems technical support personnel.
sm(spa_oir_tsm subslot 4/0 TSM), running yes, state ready
Admin Status: admin enabled,  Operational Status: ok(1)
Last reset Reason: manual
TSM Context:
    configured_spa_type 0x483
    soft remove fail code 0x0(none)
    last_fail_code 0x110E(SPA unrecognized)
    fail_count 0
    timed_fail_count 0, failed_spa_type 0x483
    recovery_action 6
    associated_fail_code 0x110E(SPA unrecognized)
    sequence numbers: next from tsm 4, last to tsm 2
    flags 0x0
Subslot:
    spa type 0x483, active spa type 0x483
    subslot flags 0x0, plugin flags 0x0
TSM Parameters:
    wait_psm_ready_timeout 360000 ms, init_timeout 240000 ms
    short_recovery_delay 5000 ms, long_recovery_delay 120000 ms
    ok_up_time 1200000 ms, bad_fail_count 10
    fail_time_period 600000 ms, max_fail_count 5
    does not support pre-configuration
SPA OIR state machine audit statistics
                In-sync poll-count  qry-fail resp-fail  restarts fail-count
subslot 4/0         yes          1         0         0         0          0
```

Related Commands

Command	Description
hw-module subslot reload	Restarts a SPA and its interfaces.
hw-module subslot shutdown	Shuts down a SPA with or without power.

show hw-module subslot service-engine status

To display the Cisco WebEx Node SPA application status on a Cisco ASR 1000 Series Router, use the **showhw-modulesubslotservice-enginestatus**command in privileged EXEC mode.

show **hw-module** **subslot** *slot*/*subslot* **service-engine** **status**

Syntax Description

slot	Specifies the chassis slot number for the Cisco ASR 1000 Series Router SIP.
/ *subslot*	Specifies the secondary subslot number on a Cisco ASR 1000 Series Router SIP where a SPA is installed.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
IOS XE Release 2.4	Thiscommand was introduced.

Usage Guidelines

Use the **showhw-modulesubslotservice-enginestatus**command to obtain information about the Cisco WebEx Node SPA application status. This includes configuration information sent from the Route Processor (RP) and the operation status of the application.

Examples

The following example provides sample output for the **showhw-modulesubslotservice-enginestatus**command for a Cisco WebEX Node SPA located in the top subslot (0) of the SIP that is installed in slot 0 on a Cisco ASR 1000 Series Router:

Related Commands

Command	Description
hw-module subslot service-engine session	Opens a session on the Cisco WebEx Node SPA console.
service-engine default-gateway	Defines a default gateway router IP address for the Cisco WebEx Node SPA.
service-engine ip address	Selects and configures the internal interface for management traffic on a Cisco WebEx Node SPA.
service-engine hostname	Specifies or modifies the hostname or domain name associated with a Cisco WebEx Node SPA.
service-engine nameserver	Specifies the primary and secondary domain name server used by the Cisco WebEx Node SPA.
service-engine wma-passcode	Configures the name and that are used for authentication on a Cisco WebEx Node SPA.

Command	Description
service-engine wma-token	Configures an encrypted token on a Cisco WebEx Node SPA.
service-engine wma-url	Specifies the URL to which the Cisco WebEx Node SPA must connect to enable WebEx meetings.

show hw-module subslot transceiver

To display the information about an optical transceiver installed in a shared port adapter (SPA), use the **showhw-modulesubslottransceiver** command in privileged EXEC configuration mode.

show hw-module subslot slot/**subslot transceiver port** {**idprom** [{**brief** | **detail** | **dump**}] | **status**}

Syntax Description

slot	Chassis slot number. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide.
/ *subslot*	Secondary slot number on a SPA interface processor (SIP) where a SPA is installed. Refer to the platform-specific SPA hardware installation guide and the corresponding "Specifying the Interface Address on a SPA" topic in the platform-specific SPA software configuration guide for subslot information.
port	Port or interface number. Refer to the platform-specific SPA hardware installation guide and the corresponding "Specifying the Interface Address on a SPA" topic in the platform-specific SPA software configuration guide for subslot information.
idprom	Displays detailed hardware information for the specified transceiver.
brief	(Optional) Displays summary hardware information for the specified transceiver.
detail	(Optional) Displays detailed hardware information for the specified transceiver.
dump	(Optional) Displays register information for the specified transceiver.
status	Displays operational status for the specified transceiver.

Command Default

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	Thiscommand was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **showhw-modulesubslottransceiver** command to obtain hardware information or operational status for optical devices installed in a SPA.

Cisco Systems qualifies the small form-factor pluggable (SFP) optics modules that can be used with SPAs.

> **Note** The SPAs will only accept the SFP modules listed as supported in this document. An SFP check is run every time an SFP module is inserted into a SPA and only SFP modules that pass this check will be usable.

If a transceiver has not been qualified by Cisco Systems for use with a SPA, the **showhw-modulesubslottransceiverstatus** command reports the following message:

```
The transceiver in slot 4 subslot 0 port 2
  is not a Cisco supplied component. In the current configuration
  third party transceivers are not serviced.
```

If a transceiver has not been qualified by Cisco Systems for use with a SPA, the**showhw-modulesubslottransceiveridprom** command reports the following message:

```
Transceiver is not a Cisco supplied part: the system cannot read the IDPROM
```

Examples

Example of the show hw-module subslot transceiver idprom Command for an OC-3 Transceiver

The following example shows hardware IDPROM information for an OC-3, short reach, multimode transceiver installed in the first interface port (0) of the SPA located in subslot 2 of the SIP installed in chassis slot 7:

```
Router# show hw-module subslot 7/2 transceiver 0 idprom

IDPROM for transceiver POS7/2/0:
  Description                               = SFP optics (type 3)
  Transceiver Type:                         = OC3 SR-1/STM1 MM (1)
  Product Indentifier (PID)                 = TRP-03BCS
  Vendor Revision                           =
  Serial Number (SN)                        = 2169298
  Vendor Name                               = OCP
  Vendor OUI (IEEE company ID)              = 00.00.00 (0)
  Device State                              = Enabled.
  CLEI code                                 = ^@^@^Cc#}0^Ll5
  Cisco part number                         = hc?z^B<@^E^R^@
  Date code (yy/mm/dd)                      = 03/04/21
  Connector type                            = LC.
  Encoding                                  = 8B10B
                                              4b5b
                                              NRZ
  Nominal bitrate                           = OC3/STM1 (200 Mbits/s)
  Minimum bit rate as % of nominal bit rate = 68 % of 200 Mbits/s
  Maximum bit rate as % of nominal bit rate = 71 % of 200 Mbits/s
```

Example of the show hw-module subslot transceiver idprom Command for an OC-12 Transceiver

The following example shows hardware IDPROM information for an OC-12, short reach, multimode transceiver installed in the first interface port (0) of the SPA located in subslot 0 of the SIP installed in chassis slot 7:

```
Router# show hw-module subslot 7/0 transceiver 0 idprom
IDPROM for transceiver POS7/0/0:
  Description                               = SFP optics (type 3)
```

```
  Transceiver Type:                          = OC12 SR-1/STM4 MM (8)
  Product Indentifier (PID)                  = TRP-12BCS
  Vendor Revision                            =
  Serial Number (SN)                         = 2177091
  Vendor Name                                = OCP
  Vendor OUI (IEEE company ID)               = 00.00.00 (0)
  Device State                               = Enabled.
  CLEI code                                  = ^@^@^CdZ+{N^\^X
  Cisco part number                          = pk:c^F^K^@
  Date code (yy/mm/dd)                       = 03/05/07
  Connector type                             = LC.
  Encoding                                   = 8B10B
                                               4b5b
                                               NRZ
  Nominal bitrate                            = OC12/STM4 (600 Mbits/s)
  Minimum bit rate as % of nominal bit rate = 92 % of 600 Mbits/s
  Maximum bit rate as % of nominal bit rate = 13 % of 600 Mbits/s
```

Example of the show hw-module subslot transceiver idprom brief Command

The following example shows the operational status of the transceiver installed in the first interface port (0) of the SPA located in subslot 2 of the SIP installed in chassis slot 3:

```
Router# show hw-module subslot 3/2 transceiver 0 idprom brief
IDPROM for transceiver POS3/2/0:
  Description                                = SFP optics (type 3)
  Transceiver Type:                          = OC12 SR-1/STM4 MM (8)
  Product Indentifier (PID)                  = TRP-12BCS
  Vendor Revision                            =
  Serial Number (SN)                         = 2569567
  Vendor Name                                = CISCO-OCP
  Vendor OUI (IEEE company ID)               = 00.00.00 (0)
  Device State                               = Enabled.
  CLEI code                                  = ^@^@^C4]  ^@T(.
  Cisco part number                          = T^W;L^YkcQ7^@
  Date code (yy/mm/dd)                       = 04/03/24
  Connector type                             = LC.
  Encoding                                   = 8B10B
                                               4b5b
                                               NRZ
  Nominal bitrate                            = OC12/STM4 (600 Mbits/s)
  Minimum bit rate as % of nominal bit rate = 92 % of 600 Mbits/s
  Maximum bit rate as % of nominal bit rate = 13 % of 600 Mbits/s
```

Example of the show hw-module subslot transceiver idprom detail Command

The following example shows the detail form of the command for the transceiver installed in the sixth interface port (5) of the SPA located in subslot 0 of the SIP installed in chassis slot 4:

```
Router# show hw-module subslot 4/0 transceiver 5 idprom detail

IDPROM for transceiver GigabitEthernet4/0/6:
  Description                                = SFP optics (type 3)
  Transceiver Type:                          = GE SX (19)
  Product Indentifier (PID)                  = FTRJ8519P1BNL-C3
  Vendor Revision                            = A1
  Serial Number (SN)                         = FNS0821K2J5
  Vendor Name                                = CISCO-FINISAR
```

```
Vendor OUI (IEEE company ID)              = 00.90.65 (36965)
CLEI code                                 = CNUIAAMAAA
Cisco part number                         = 10-1954-01
Device State                              = Enabled.
Date code (yy/mm/dd)                      = 04/05/19
Connector type                            = LC.
Encoding                                  = 8B10B
                                            NRZ
Nominal bitrate                           = 2xFC (2100 Mbits/s)
Minimum bit rate as % of nominal bit rate = not specified
Maximum bit rate as % of nominal bit rate = not specified
Link reach for 9u fiber (km)              = SX(550/270m) (0)
                                            1xFC-MM(500/300m) (0)
                                            2xFC-MM(300/150m) (0)
                                            ESCON-MM(2km) (0)
Link reach for 9u fiber (m)               = SX(550/270m) (0)
                                            1xFC-MM(500/300m) (0)
                                            2xFC-MM(300/150m) (0)
                                            ESCON-MM(2km) (0)
Link reach for 50u fiber (m)              = 2xFC-MM(300/150m) (30)
Link reach for 62.5u fiber (m)            = 2xFC-MM(300/150m) (15)
Nominal laser wavelength                  = 850 nm.
DWDM wavelength fraction                  = 850.0  nm.
Supported options                         = Tx disable
                                            Tx fault signal
                                            Loss of signal (standard implementation)
Supported enhanced options                = Alarms for monitored parameters
Diagnostic monitoring                     = Digital diagnostics supported
                                            Diagnostics are externally calibrated
                                            Rx power measured is "Averagepower"
Transceiver temperature operating range   = -5 C to 85 C (extended)
Minimum operating temperature             = -20 C
Maximum operating temperature             = 90 C
High temperature alarm threshold          = +109.000 C
High temperature warning threshold        = +103.000 C
Low temperature warning threshold         =  -13.000 C
Low temperature  alarm threshold          =  -29.000 C
High voltage alarm threshold              = 3.9000 Volts
High voltage warning threshold            = 3.7000 Volts
Low voltage warning threshold             = 2.9000 Volts
Low voltage alarm threshold               = 2.7000 Volts
High laser bias current alarm threshold   = 15.000 mAmps
High laser bias current warning threshold = 12.000 mAmps
Low laser bias current warning threshold  = 2.000 mAmps
Low laser bias current alarm threshold    = 1.000 mAmps
High transmit power alarm threshold       = 0.7424 mWatts
High transmit power warning threshold     = 0.7424 mWatts
Low transmit power warning threshold      = 0.959 mWatts
Low transmit power alarm threshold        = 0.619 mWatts
High receive power alarm threshold        = 5.9324 mWatts
High receive power warning threshold      = 3.7416 mWatts
Low receive power warning threshold       = 0.751 mWatts
Low receive power alarm threshold         = 0.478 mWatts
External Calibration constant: Rx power4  = 0.000
External Calibration constant: Rx power3  = 0.000
External Calibration constant: Rx power2  = 0.000
External Calibration constant: Rx power1  = 0.212
External Calibration constant: Rx power0  = -1.4294966868
External Calibration: bias current slope  = 1.000
External Calibration: bias current offset = 0
```

Example of the show hw-module subslot transceiver status Command

The following example shows the operational status of the transceiver installed in the third interface port (2) of the SPA located in subslot 0 of the SIP installed in chassis slot 4:

```
Router# show hw-module subslot 4/0 transceiver 2 status
The Transceiver in slot 4 subslot 0 port 2 is enabled.
  Module temperature                = +41.617 C
  Transceiver Tx supply voltage     = 3292.0 uVolts
  Transceiver Tx bias current       = 4840 uAmps
  Transceiver Tx power              = 349.2 uWatts
  Transceiver Rx optical power      = 0.5 uWatts
```

show hw-programmable

To display the current Complex Programmable Logic Device (CPLD) or Field-Programmable Gate Array (FPGA) version in a particular line card on a Cisco ASR 1000 Series Router, use the **showhw-programmable** command in Privileged EXEC configuration mode.

show hw-programmable {**all** | **R0** | **R1** | **F0** | **F1** | **0 . . 5**}

Syntax Description

all	This selects all line card types in a Cisco ASR 1000 Series Router.
R0	RP slot 0. In the Cisco ASR 1006 Routers and Cisco ASR 1013 Routers, it is the lower RP slot. In Cisco ASR 1002 and Cisco ASR 1004, it is the only slot.
R1	RP slot 1. This is only in the Cisco ASR 1006 and Cisco ASR 1013 Routers. It is the higher RP slot.
F0	This is the embedded services processor (ESP) slot 0. In the Cisco ASR 1006 Routers and Cisco ASR 1013 Routers, it is the lower ESP slot. In Cisco ASR 1002 and Cisco ASR 1004, it is the only slot.
F1	This is the embedded services processor (ESP) slot 2. This is only in the Cisco ASR 1006 and Cisco ASR 1013 Routers. It is the higher ESP slot.
0..5	This is one of the SIP carrier card slots. Select a slot number zero (0) through five (5). **Note** A CPLD upgrade cannot be performed in slot 5 in the ASR100-SIP10. Move the CPLD card to another slot.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
3.1S	This command was introduced in Cisco IOS XE Release 3.1S.

Usage Guidelines

This command displays the current CPLD and FPGA versions in a particular card by examining the contents of the hw-programmable package file.

For procedures on performing a CPLD upgrade, see the Upgrading Field Programmable Hardware Devices for Cisco ASR 1000 Series Routers document.

Examples

The following example displays the current CPLD and FPGA versions in slot R0 of the router:

```
Router# show hw-programmable r0
Hw-programmable versions

Slot                CPLD version               FPGA version
-----------------------------------------------------------
R0                  10021901                   08112501
```

The following example displays all CPLD and FPGA versions, including RP, ESP, and SIP carrier card:

```
Router# show hw-programmable all
Hw-programmable versions

Slot              CPLD version              FPGA version
-----------------------------------------------------------
R0                10021901                  08112501
R1                N/A                       N/A
F0                1001270D                  09081902
F1                1003190E                  10040702
1                 07091401                  N/A
2                 07091401                  N/A
3                 07091401                  N/A
4                 07091401                  N/A
5                 07091401                  N/A
```

Related Commands

Command	Description
upgrade hw-programmable	Performs a Complex Programmable Logic Device (CPLD) or Field-Programmable Gate Array (FPGA) upgrade on a Cisco ASR 1000 Series Router.
show upgrade hw-programmable progress	Displays the progress of the line card-field upgradeable device (LC-FPD) on a Cisco ASR 1000 Series Router.
show upgrade hw-programmable	Displays the names and versions of individual files in the hw_programmable package file.

show icc

To display the information about the interface controller card (ICC) counter and status, use the **showicc** command in user EXEC or privileged EXEC mode.

show icc {**counters** | **flowcontrol** | **mcast** | **status**}

Syntax Description

counters	Displays the counter information.
flowcontrol	Displays the flow control information.
mcast	Displays the multicast information.
status	Displays the status information.

Command Default

This command has no default settings.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to display the information about the ICC counter:

```
Router>
show icc counters
total tx RPC packets to slot 1 LCP = 0
  detail by request id: (<request-id>=<number-of-packets>)
   2 =0            7 =0            8 =0            10=0
   11=0            12=0            14=0            17=0
   18=0            19=0            20=0
total rx RPC packets from slot 1 LCP = 0
  detail by request id: (<request-id>=<number-of-packets>)
   2 =5            7 =7            8 =11           10=4
   11=1            12=2            14=1            17=67
   18=7            19=159          20=29
total tx MCAST-SP packets to slot 1 LCP = 0
  detail by request id: (<request-id>=<number-of-packets>)
   6 =0            7 =0            8 =0            9 =0
   12=0            14=0
total rx MCAST-SP packets from slot 1 LCP = 0
  detail by request id: (<request-id>=<number-of-packets>)
   6 =1            7 =1            8 =1            9 =1
   12=41           14=67
total tx L3-MGR packets to slot 1 LCP = 0
  detail by request id: (<request-id>=<number-of-packets>)
   1 =0            2 =0            3 =0
total rx L3-MGR packets from slot 1 LCP = 0
```

```
  detail by request id: (<request-id>=<number-of-packets>)
   1 =1            2 =2            3 =1
Router#
```

This example shows how to display the information about the ICC status:

```
Router>
show icc status
Class Name             Msgs Pending  Max Pending  Total Sent
----- ---------------- ------------  -----------  ----------
    2 RPC                         0            3         403
    3 MSC                         0            1           1
    5 L3-MGR                      0            4        4173
   13 TCAM-API                    0           10          26
Router#
```

Related Commands

Command	Description
show interfaces	Displays the status and statistics for the interfaces in the chassis.

show interfaces cem

T o display the statistics of the cem group, use the **showinterfacescem**commandin privilege exec mode.

show interfaces cem *slot/subslot/port*

Syntax Description

slot	Slot number where the SIP is installed.
subslot	Subslot number of the SIP where CEOPS SPA has been installed and circuit emulation has been configured.
port	Port number of the interface on the CEOPS SPA where circuit emulation has been configured.

Command Default

No default behavior or values

Command Modes

Privilege Exec Mode (Exec)

Command History

Release	Modification
Cisco IOS XE Release 3.3.0S	This command was introduced.

Usage Guidelines

The **showinterfacescem**command has been introduced on Cisco ASR 1000 Series Router in Cisco IOS XE Release 3.3.0S. The command output provides details regarding the various CEM groups configured and the various time slots to which the groups are attached.

Examples

The following example shows the command output of the show interfaces cem command:

```
Router# show interfaces cem 0/1/0
CEM0/1/0 is up, line protocol is up
  Hardware is Circuit Emulation Interface
  MTU 1500 bytes, BW 155520 Kbit/sec, DLY 0 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation CEM, loopback not set
  Keepalive not supported
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 64000 bits/sec, 250 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1779066 packets input, 56930112 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
```

Related Commands

Command	Description
clear interface cem	Clears the cem channel.

show interface history

To display histograms of interface utilization, use the **showinterfacehistory** command in privileged EXEC mode.

show interface [*type number*] **history** [{**all** | **60sec** | **60min** | **72hour**}] [{**both** | **input** | **output**}]

Syntax Description

type	(Optional) Interface type.
number	(Optional) Port number of the interface.
all	(Optional) Specifies the histograms representing the last 60 seconds, the last 60 minutes, and the last 72 hours of interface utilization.
60sec	(Optional) Specifies the histograms representing the last 60 seconds of interface utilization.
60min	(Optional) Specifies the histograms representing the last 60 minutes of interface utilization.
72hour	(Optional) Specifies the histograms representing the last 72 hours of interface utilization.
both	(Optional) Specifies both the input histograms and the output histograms.
input	(Optional) Specifies the input histograms.
output	(Optional) Specifies the output histograms.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)XNE	This command was introduced.

Usage Guidelines

The **showinterfacehistory** command displays histograms of interface utilization. The y-axis represents the input or output rate in packets per second, kilobits per second, or megabits per second. Kilobits per second is used when the bandwidth of the interface is less than one gigabit per second. Megabits per second is used for more than one gigabit per second.

The x-axis represents time in units of seconds, minutes or hours with the most current time at the left side of the histogram. There are three histograms available: the last 60 seconds, the last 60 minutes, and the last 72 hours.

The interface counters specified in the **history(interface)** command are displayed under the x-axis of each histogram. Each counter has a five-character identification as listed in the command. The identification is displayed at the beginning of each counter line. The number in the column indicates that the counter incremented by that amount during the specified interval. When the counter exceeds a single digit, the values are displayed vertically.

Examples

The following example shows the histogram output of interface history:

```
Router# show interface gigabitethernet 0/1 history 60min
```

```
5689688755455324777665666876546
      10
       9    *
       8   ** **                  *
       7   *# ##*        ***      #*
       6  *######        ####* **###*  *
       5 ########## *#   ############* *
       4 #############  *#############**
       3 ############## ###############*
       2 ###############################
       1 ###############################
        0....5....1....1....2....2....3....3....4....4....5....5....6
                  0    5    0    5    0    5    0    5    0    5    0
         3333333333333333333333333333331
   Mlcst 556555555565555555555565535555700000000000000000000000000000
         22322111111     121221211211
         57149774766867 133175814422022
   iDrop 425727636924219265454496840996600000000000000000000000000000
         GigabitEthernet0/1 input rate(mbits/sec)  (last 60 minutes)
                 * = maximum   # = average
5677678656555434767665666866545
      10
       9
       8       *                  *
       7   ** *#         * *      *
       6  *#####* *      ##*** ***##*
       5 *#########***   #####*######* *
       4 #############* *#############**
       3 #############**###############*
       2 ###############################
       1 ###############################
        0....5....1....1....2....2....3....3....4....4....5....5....6
                  0    5    0    5    0    5    0    5    0    5    0
   Unkno 000000000000000000000000000000000000000000000000000000000000
   oDrop 000000000000000000000000000000000000000000000000000000000000
         GigabitEthernet0/1 output rate(mbits/sec)  (last 60 minutes)
                 * = maximum   # = average
```

The input rate histogram shows that the input rate peaked at 9 Mbps and 4 minutes prior to the command execution. During that one-minute interval, there were 35 input multicast packets and 247 input drops. The counter values in the histogram should be read vertically.

The output rate histogram shows that the output rate reached 8 Mbps twice; once 7 minutes prior and the second time 26 minutes prior to the command execution. There were no unknown protocol drops and no output drops during the last 60 minutes.

The table below describes the significant fields shown in the display.

Table 112: show interface history Field Descriptions

Field	Description
Mlcst	Ethernet input multicast.
iDrop	Input drops.
Unkno	Unknown protocol drops.
oDrop	Output drops.

Related Commands

Command	Description
history (interface)	Enables an interface to maintain utilization history.

show interface sdcc

To display configuration information and statistics for a sections data communications channel (SDCC) interface, use the **showinterfacesdcc** command in privileged EXEC mode.

show interface sdcc *slot/subslot/port*

Syntax Description

slot	Chassis slot number. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding “Identifying Slots and Subslots for SIPs and SPAs” topic in the platform-specific SPA software configuration guide.
/ *subslot*	Secondary slot number on a SPA interface processor (SIP) where a SPA is installed. Refer to the platform-specific SPA hardware installation guide and the corresponding “Specifying the Interface Address on a SPA” topic in the platform-specific SPA software configuration guide for subslot information.
/ *port*	(Optional) Port or interface number. Refer to the appropriate hardware manual for port information. For SPAs, refer to the corresponding “Specifying the Interface Address on a SPA” topics in the platform-specific SPA software configuration guide.

Command Default

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)BC3	This command was introduced.
12.2(25)S3	This command was integrated into Cisco IOS Release 12.2(25)S3 to support POS SPAs on the Cisco 7304 router.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE to support POS SPAs on the Cisco 7600 series routers and Catalyst 6500 series switches.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S to support POS SPAs on the Cisco 12000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

Cisco 7600 Series Router and Catalyst 6500 Series Switch Example

The following command displays configuration information and statistics for SDCC interface 7/0/0:

```
Router# show interface sdcc 7/0/0
SDCC7/0/0 is up, line protocol is up
```

```
  Hardware is SDCC
  Internet address is 10.11.11.10/8
  MTU 1500 bytes, BW 192 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, crc 16, loopback not set
  Keepalive not set
  Last input 00:00:38, output 00:00:38, output hang never
  Last clearing of "show interface" counters 00:00:48
  Input queue:0/75/0/0 (size/max/drops/flushes); Total output drops:0
  Queueing strategy:fifo
  Output queue:0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     5 packets input, 520 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     5 packets output, 520 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
```

Cisco 12000 Series Router Example

The following is sample output from the **showinterfacesdcc**command on a Cisco 12000 series router for POS interface 1/1/0 (which is the interface for port 0 of the SPA in subslot 1 of the SIP in chassis slot 1):

```
Router# show interface sdcc 1/1/0

SDCC1/1/0 is administratively down, line protocol is down
  Hardware is SDCC
  MTU 1500 bytes, BW 192 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, crc 32, loopback not set
  Keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 00:01:55
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
```

The table below describes the significant fields shown in these displays.

*Table 113: **show interface sdcc** Field Descriptions*

Field	Description
SDCCx/y/z is up, line protocol is up	Indicates whether the interface hardware is currently active and can transmit and receive or whether it has been taken down by an administrator.

Field	Description
Hardware is. . .	Hardware type: • SDCC-- Section Data Communications Channel
Internet address is	Internet address and subnet mask.
MTU	Maximum transmission unit of the interface.
BW	Bandwidth of the interface, in kilobits per second.
DLY	Delay of the interface, in microseconds.
rely	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes. The calculation uses the value from the **bandwidth** interface configuration command.
Encapsulation	Encapsulation method assigned to interface.
crc	Cyclic redundancy check size (16 or 32 bits).
Loopback	Indicates whether loopback is set.
Keepalive	Indicates whether keepalives are set.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This counter is updated only when packets are process-switched, not when packets are fast-switched.
(Last) output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by an interface. This counter is updated only when packets are process-switched, not when packets are fast-switched.
(Last) output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the “last” fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. *** indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 2231 ms (and less than 232 ms) ago.
Queueing strategy	First-in, first-out (FIFO) queueing strategy (other queueing strategies you might see are priority-list, custom-list, and weighted fair).

Field	Description
Output queue, drops input queue, drops	Number of packets in output and input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped because a queue was full.
5 minute input rate 5 minute output rate	Average number of bits and packets received or transmitted per second in the last 5 minutes.
packets input	Total number of error-free packets received by the system.
bytes (input)	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernets and bursts of noise on serial lines are often responsible for no input buffer events.
broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium.
throttles	Not supported for POS interfaces.
parity	Report of the parity errors on the interface.
input errors	Total number of no buffer, runts, giants, CRCs, frame, overrun, ignored, and abort counts. Other input-related errors can also increment the count, so that this sum might not balance with the other counts.
CRC	Cyclic redundancy checksum generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data. On a serial link, CRCs usually indicate noise, gain hits or other transmission problems on the data link.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a serial line, this is usually the result of noise or other transmission problems.
overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be incremented.

Field	Description
abort	Illegal sequence of one bits on the interface.
packets output	Total number of messages transmitted by the system.
bytes (output)	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the far-end transmitter has been running faster than the near-end router’s receiver can handle.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this might not balance with the sum of the enumerated output errors, as some datagrams can have more than one error, and others can have errors that do not fall into any of the specifically tabulated categories.
collisions	Not supported for POS interfaces.
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within a certain interval. If the system notices that the carrier detect line of an interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an unrecoverable interface processor error occurred, or when an interface is looped back or shut down.
output buffer failures	Not supported for POS interfaces.
output buffers swapped out	Not supported for POS interfaces.
carrier transitions	Number of times the carrier detect signal of the interface has changed state.

show interfaces

To display statistics for all interfaces configured on the router or access server, use the **show interfaces** command in privileged EXEC mode.

Cisco 2500 Series, Cisco 2600 Series, Cisco 4700 Series, and Cisco 7000 Series
show interfaces [*type number*] [*first*] [*last*] [**accounting**]

Catalyst 6500 Series, Cisco 7200 Series and Cisco 7500 Series with a Packet over SONET Interface Processor
show interfaces [**type slot/port**] [{**accounting** | **counters protocol status** | **crb** | **dampening** | **description** | **dot1ad** | **etherchannel** [**module number**] | **fair-queue** | **irb** | **mac-accounting** | **mpls-exp** | **precedence** | **random-detect** | **rate-limit** | **stats** | **summary** | **switching** | **utilization** {*type number*}}]

Cisco 7500 Series with Ports on VIPs
show interfaces [*type slot/port-adapter/port*]

Cisco 7600 Series
show interfaces [{*type number* | **null** *interface-number* | **vlan** *vlan-id*}]

Channelized T3 Shared Port Adapters
show interfaces serial [*slot/subslot/port/t1-num* **:** *channel-group*]

Shared Port Adapters
show interfaces type [*slot/subslot/port* [*/sub-int*]]

Syntax Description

type	(Optional) Interface type. Allowed values for *type* can be **atm**, **async**, **auto-template**, **bvi**, **bri0**, **ctunnel**, **container**, **dialer**, **e1**, **esconPhy**, **ethernet**, **fastethernet**, **fcpa**, **fddi**, **filter**, **filtergroup**, **gigabitethernet**, **ge-wan**, **hssi**, **longreachethernet**, **loopback**, **mfr**, **multilink**, **module**,**null**, **posport-channel**, , **port-group**, **pos-channel**, **sbc**, **sdcc**, **serial**, **sysclock**, **t1**, **tengigabitethernet**, **token**, **tokenring**, **tunnel**, **vif**, **vmi**, **virtual-access**, **virtual-ppp**, **virtual-template**, **virtual-tokenring**. **voaBypassIn**, **voaBypassOut**, **voaFilterIn**, **voaFilterOut**, **voaIn**, **voaOut**. **Note** The type of interfaces available is based on the type of router used.
number	(Optional) Port number on the selected interface.
first last	(Optional) For Cisco 2500 series routers, ISDN Basic Rate Interfae (BRI) only. The *first* argument can be either 1 or 2. The *last* argument can only be 2, indicating B channels 1 and 2. D-channel information is obtained by using the command without the optional arguments.
accounting	(Optional) Displays the number of packets of each protocol type that have been sent through the interface.

counters protocol status	(Optional) Displays the current status of the protocol counters enabled.
crb	(Optional) Displays interface routing or bridging information.
dampening	(Optional) Displays interface dampening information.
description	(Optional) Displays the interface description.
etherchannel [**module***number*]	(Optional) Displays interface Ether Channel information. • **module** --The **module** keyword limits the display to interfaces available on the module.
fair-queue	(Optional) Displays interface Weighted Fair Queueing (WFQ) information.
irb	(Optional) Displays interface routing or bridging information.
mac-accounting	(Optional) Displays interface MAC accounting information.
mpls-exp	(Optional) Displays interface Multiprotocol Label Switching (MPLS) experimental accounting information.
precedence	(Optional) Displays interface precedence accounting information.
random-detect	(Optional) Displays interface Weighted Random Early Detection (WRED) information.
rate-limit	(Optional) Displays interface rate-limit information.
stats	(Optional) Displays interface packets and octets, in and out, by using switching path.
summary	(Optional) Displays an interface summary.
switching	(Optional) Displays interface switching.
null *interface-number*	(Optional) Specifies the null interface, that is **0**.
slot	(Optional) Slot number. Refer to the appropriate hardware manual for slot information.
/ *port*	(Optional) Port number. Refer to the appropriate hardware manual for port information.
/ *port-adapter*	(Optional) Port adapter number. Refer to the appropriate hardware manual for information about port adapter compatibility.

slot / *subslot* / *port* / *t1-num* **:** *channel-group*	(Optional) Channelized T3 Shared Port Adapters Number of the chassis slot that contains the channelized T3 Shared Port Adapters (SPA) (for example, 5/0/0:23), where: • *slot* --(Optional) Chassis slot number. For SPA interface processors (SIPs), refer to the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide. • / *subslot*-- (Optional) Secondary slot number on a SIP where a SPA is installed. Refer to the platform-specific SPA hardware installation guide and the corresponding "Specifying the Interface Address on a SPA" topic in the platform-specific SPA software configuration guide for subslot information. • / *port* --(Optional) Port or interface number. For SPAs, refer to the corresponding "Specifying the Interface Address on a SPA" topic in the platform-specific SPA software configuration guide. • / *t1-num*-- (Optional) T1 time slot in the T3 line. The value can be from 1 to 28. • **:** *channel-group*-- (Optional) Number 0-23 of the DS0 link on the T1 channel.
[*slot*/*subslot*/*port*/*sub-int*]]	(Optional) Shared Port Adapters Number of the chassis slot that contains the SPA interface (for example, 4/3/0), where: • *slot* --(Optional) Chassis slot number. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide. • / *subslot*-- (Optional)Secondary slot number on a SIP where a SAP is installed. Refer to the platform-specific SPA hardware installation guide and the corresponding "Specifying the Interface Address on a SPA" topic in the platform-specific SPA software configuration guide for subslot information. • / *port* --(Optional) Port or interface number. For SPAs, refer to the corresponding "Specifying the Interface Address on a SPA" topics in the platform-specific SPA software configuration guide. • / *sub-int* -- (Optional) Subinterface number (for those SPAs that support subinterface configuration).
vlan *vlan-id*	(Optional) Specifies the VLAN ID; valid values are from 1 to 4094.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.0(3)T	This command was modified to include support for flow-based WRED .
12.0(4)T	This command was modified to include enhanced display information for dialer bound interfaces.
12.0(7)T	This command was modified to include **dialer** as an interface type and to reflect the default behavior.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(20)S2	This command was integrated into Cisco IOS Release 12.2(20)S2 and introduced a new address format and output for SPA interfaces on the Cisco 7304 router. The *subslot* argument was introduced.
12.2(25)S3	This command was integrated into Cisco IOS Release 12.2(25)S3.
12.2(14)SX	This command was modified. Support for this command was added for the Supervisor Engine 720.
12.2(17d)SXB	This command was modified. Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2SX. The uplink dual-mode port information was updated.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE to support SPAs on the Cisco 7600 series routers and Catalyst 6500 series switches.
2.2(33)SXJ01	This command was integrated into Cisco IOS Release 12.2(33)SXJ01.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S to support SPAs on the Cisco 12000 series routers, and the **tengigabitethernet** interface type was added. 10-Gigabit Ethernet interfaces were introduced with the release of the 1-Port 10-Gigabit Ethernet SPA.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB1	This command was updated to display operational status for Gigabit Ethernet interfaces that are configured as primary and backup interfaces (Cisco 7600 series routers).
12.2(31)SB	This command was integrated in Cisco IOS Release 12.2(31)SB.
12.2(33)SB	This command was modified. The default value of the command was modified on the Cisco 10000 series router for the PRE3 and PRE4.

Release	Modification
Cisco IOS XE Release 2.5	This command was implemented on Cisco ASR 1000 Series Aggregation Services Routers.
12.2(50)SY	This command was integrated in Cisco IOS Release 12.2(50)SY and the dot1ad keyword was added.
15.1(01)SY	This command was integrated in Cisco IOS Release 15.1(50)SY.

Usage Guidelines

Display Interpretation

The **show interfaces** command displays statistics for the network interfaces. The resulting output varies, depending on the network for which an interface has been configured. The resulting display on the Cisco 7200 series routers shows the interface processors in slot order. If you add interface processors after booting the system, they will appear at the end of the list, in the order in which they were inserted.

Information About Specific Interfaces

The *number* argument designates the module and port number. If you use the **show interfaces** command on the Cisco 7200 series routers without the *slot/port* arguments, information for all interface types will be shown. For example, if you type **show interfaces** you will receive information for all Ethernet, serial, Token Ring, and FDDI interfaces. Only by adding the type *slot/port* argument you can specify a particular interface.

Cisco 7600 Series Routers

Valid values for the *number* argument depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

The port channels from 257 to 282 are internally allocated and are supported on the Content Switching Module (CSM) and the Firewall Services Module (FWSM) only.

Statistics are collected on a per-VLAN basis for Layer 2-switched packets and Layer 3-switched packets. Statistics are available for both unicast and multicast traffic. The Layer 3-switched packet counts are available for both ingress and egress directions. The per-VLAN statistics are updated every 5 seconds.

In some cases, you might see a difference in the duplex mode that is displayed between the **show interfaces** command and the **show running-config**commands. In this case, the duplex mode that is displayed in the **show interfaces** command is the actual duplex mode that the interface is running. The **show interfaces** command shows the operating mode for an interface, and the **show running-config** command shows the configured mode for an interface.

If you do not enter any keywords, all counters for all modules are displayed.

Command Variations

You will use the **show interfaces** command frequently while configuring and monitoring devices. The various forms of the **show interfaces** commands are described in detail in the sections that follow.

Dialer Interfaces Configured for Binding

If you use the **show interfaces** command on dialer interfaces configured for binding, the display will report statistics on each physical interface bound to the dialer interface; see the following examples for more information.

Removed Interfaces

If you enter a **show interfaces** command for an interface type that has been removed from the router or access server, interface statistics will be displayed accompanied by the following text: "Hardware has been removed."

Weighted Fair Queueing Information

If you use the **show interfaces** command on a router or access server for which interfaces are configured to use weighted fair queueing through the **fair-queue** interface command, additional information is displayed. This information consists of the current and high-water mark number of flows.

Cisco 10000 Series Router

In Cisco IOS Release 12.2(33)SB, when a multilink PPP (MLP) interface is down/down, its default bandwidth rate is the sum of the serial interface bandwidths associated with the MLP interface.

In Cisco IOS Release 12.2(31)SB, the default bandwidth rate is 64 Kbps.

Examples

The following is sample output from the **show interfaces** command. Because your display will depend on the type and number of interface cards in your router or access server, only a portion of the display is shown.

Note If an asterisk (*) appears after the throttles counter value, it means that the interface was throttled at the time the command was run.

```
Router# show interfaces
Ethernet 0 is up, line protocol is up
  Hardware is MCI Ethernet, address is 0000.0c00.750c (bia 0000.0c00.750c)
  Internet address is 10.108.28.8, subnet mask is 255.255.255.0
  MTU 1500 bytes, BW 10000 Kbit, DLY 100000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 4:00:00
  Last input 0:00:00, output 0:00:00, output hang never
  Last clearing of "show interface" counters 0:00:00
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  Five minute input rate 0 bits/sec, 0 packets/sec
  Five minute output rate 2000 bits/sec, 4 packets/sec
     1127576 packets input, 447251251 bytes, 0 no buffer
     Received 354125 broadcasts, 0 runts, 0 giants, 57186* throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     5332142 packets output, 496316039 bytes, 0 underruns
     0 output errors, 432 collisions, 0 interface resets, 0 restarts
.
.
.
```

Example with Custom Output Queueing

The following example shows partial sample output when custom output queueing is enabled:

```
Router# show interfaces
Last clearing of "show interface" counters 0:00:06
Input queue: 0/75/0 (size/max/drops); Total output drops: 21
Output queues: (queue #: size/max/drops)
     0: 14/20/14  1: 0/20/6  2: 0/20/0 3: 0/20/0 4: 0/20/0 5: 0/20/0
     6: 0/20/0 7: 0/20/0  8: 0/20/0  9: 0/20/0  10: 0/20/0
.
```

.
.

When custom queueing is enabled, the drops accounted for in the output queues result from bandwidth limitation for the associated traffic and lead to queue length overflow. Total output drops include drops on all custom queues and the system queue. Fields are described with the weighted fair queueing output in the table below.

Example Including Weighted-Fair-Queueing Output

For each interface on the router or access server configured to use weighted fair queueing, the **show interfaces** command displays the information beginning with *Inputqueue***:** in the following display:

```
Router# show interfaces
Ethernet 0 is up, line protocol is up
  Hardware is MCI Ethernet, address is 0000.0c00.750c (bia 0000.0c00.750c)
  Internet address is 10.108.28.8, subnet mask is 255.255.255.0
  MTU 1500 bytes, BW 10000 Kbit, DLY 100000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 4:00:00
  Last input 0:00:00, output 0:00:00, output hang never
  Last clearing of "show interface" counters 0:00:00
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  Five minute input rate 0 bits/sec, 0 packets/sec
  Five minute output rate 2000 bits/sec, 4 packets/sec
     1127576 packets input, 447251251 bytes, 0 no buffer
     Received 354125 broadcasts, 0 runts, 0 giants, 57186* throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     5332142 packets output, 496316039 bytes, 0 underruns
     0 output errors, 432 collisions, 0 interface resets, 0 restarts
Input queue: 0/75/0 (size/max/drops); Total output drops: 0
Output queue: 7/64/0 (size/threshold/drops)
         Conversations 2/9 (active/max active)
```

The table below describes the input queue and output queue fields shown in the preceding two displays.

Table 114: Weighted-Fair-Queueing Output Field Descriptions

Field	Description
Input Queue	
size	Current size of the input queue.
max	Maximum size of the queue.
drops	Number of messages discarded in this interval.
Total output drops	Total number of messages discarded in this session.
Output Queue	
size	Current size of the output queue.
threshold	Congestive-discard threshold. Number of messages in the queue after which new messages for high-bandwidth conversations are dropped.

Field	Description
drops	Number of dropped messages.
Conversations: active	Number of currently active conversations.
Conversations: max active	Maximum number of concurrent conversations allowed.

Example with Accounting Option

To display the number of packets of each protocol type that have been sent through all configured interfaces, use the **show interfaces accounting** command. When you use the **accounting** option, only the accounting statistics are displayed.

Note Except for protocols that are encapsulated inside other protocols, such as IP over X.25, the accounting option also shows the total bytes sent and received, including the MAC header. For example, it totals the size of the Ethernet packet or the size of a packet that includes High-Level Data Link Control (HDLC) encapsulation.

Per-packet accounting information is kept for the following protocols:

- AppleTalk
- Address Resolution Protocol (ARP) (for IP, Frame Relay, Switched Multimegabit Data Service (SMDS))
- Connectionless Network Service (CLNS)
- Digital Equipment Corporation (DEC) Maintenance Operations Protocol (MOP)

The routers use MOP packets to advertise their existence to Digital Equipment Corporation machines that use the MOP. A router periodically broadcasts MOP packets to identify itself as a MOP host. This results in MOP packets being counted, even when DECnet is not being actively used.

- DECnet
- HP Probe
- IP
- LAN Manager (LAN Network Manager and IBM Network Manager)
- Novell
- Serial Tunnel Synchronous Data Link Control (SDLC)
- Spanning Tree
- SR Bridge
- Transparent Bridge

Example with DWRED

The following is sample output from the **show interfaces** command when distributed WRED (DWRED) is enabled on an interface. Notice that the packet drop strategy is listed as “VIP-based weighted RED.”

```
Router# show interfaces hssi 0/0/0
Hssi0/0/0 is up, line protocol is up
  Hardware is cyBus HSSI
  Description: 45Mbps to R1
Internet address is 10.200.14.250/30
MTU 4470 bytes, BW 45045 Kbit, DLY 200 usec, rely 255/255, load 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
Last input 00:00:02, output 00:00:03, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Packet Drop strategy: VIP-based weighted RED
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
1976 packets input, 131263 bytes, 0 no buffer
Received 1577 broadcasts, 0 runts, 0 giants
0 parity
4 input errors, 4 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
1939 packets output, 130910 bytes, 0 underruns
0 output errors, 0 applique, 3 interface resets
0 output buffers copied, 0 interrupts, 0 failures
```

Example with ALC

The following is sample output from the **show interfaces** command for serial interface 2 when Airline Control (ALC) Protocol is enabled:

```
Router# show interfaces serial 2
Serial2 is up, line protocol is up
Hardware is CD2430
MTU 1500 bytes, BW 115 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation ALC, loopback not set
Full-duplex enabled.
     ascus in UP state: 42, 46
     ascus in DOWN state:
     ascus DISABLED:
Last input never, output never, output hang never
Last clearing of “show interface” counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 3 interface resets
0 output buffer failures, 0 output buffers swapped out
DCD=down  DSR=down  DTR=down  RTS=down  CTS=down
```

Example with SDLC

The following is sample output from the **show interfaces** command for an SDLC primary interface supporting the SDLC function:

```
Router# show interfaces
Serial 0 is up, line protocol is up
 Hardware is MCI Serial
 MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
 Encapsulation SDLC-PRIMARY, loopback not set
      Timers (msec): poll pause 100 fair poll 500. Poll limit 1
      [T1 3000, N1 12016, N2 20, K 7] timer: 56608 Last polled device: none
      SDLLC [ma: 0000.0C01.14--, ring: 7 bridge: 1, target ring: 10
             largest token ring frame 2052]
SDLC addr C1 state is CONNECT
       VS 6, VR 3, RCNT 0, Remote VR 6, Current retransmit count 0
       Hold queue: 0/12 IFRAMEs 77/22 RNRs 0/0 SNRMs 1/0 DISCs 0/0
       Poll: clear, Poll count: 0, chain: p: C1 n: C1
       SDLLC [largest SDLC frame: 265, XID: disabled]
  Last input 00:00:02, output 00:00:01, output hang never
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  Five minute input rate 517 bits/sec, 30 packets/sec
  Five minute output rate 672 bits/sec, 20 packets/sec
       357 packets input, 28382 bytes, 0 no buffer
       Received 0 broadcasts, 0 runts, 0 giants
       0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
       926 packets output, 77274 bytes, 0 underruns
       0 output errors, 0 collisions, 0 interface resets, 0 restarts
       2 carrier transitions
```

The table below shows the fields relevant to all SDLC connections.

*Table 115: **show interfaces** Field Descriptions When SDLC Is Enabled*

Field	Description
Timers (msec)	List of timers in milliseconds.
poll pause, fair poll, Poll limit	Current values of these timers.
T1, N1, N2, K	Current values for these variables.

The table below shows other data given for each SDLC secondary interface configured to be attached to this interface.

Table 116: SDLC Field Descriptions

Field	Description
addr	Address of this secondary interface.

Field	Description
State	Current state of this connection. The possible values follow: • BOTHBUSY--Both sides have told each other that they are temporarily unable to receive any more information frames. • CONNECT--A normal connect state exists between this router and this secondary. • DISCONNECT--No communication is being attempted to this secondary. • DISCSENT--This router has sent a disconnect request to this secondary and is awaiting its response. • ERROR--This router has detected an error, and is waiting for a response from the secondary acknowledging this. • SNRMSENT--This router has sent a connect request (SNRM) to this secondary and is awaiting its response. • THEMBUSY--This secondary has told this router that it is temporarily unable to receive any more information frames. • USBUSY--This router has told this secondary that it is temporarily unable to receive any more information frames.
VS	Sequence number of the next information frame this station sends.
VR	Sequence number of the next information frame from this secondary that this station expects to receive.
RCNT	Number of correctly sequenced I-frames received when the Cisco IOS software was in a state in which it is acceptable to receive I-frames.
Remote VR	Last frame transmitted by this station that has been acknowledged by the other station.
Current retransmit count	Number of times the current I-frame or sequence of I-frames has been retransmitted.
Hold queue	Number of frames in hold queue/Maximum size of hold queue.
IFRAMEs, RNRs, SNRMs, DISCs	Sent and received count for these frames.
Poll	“Set” if this router has a poll outstanding to the secondary; “clear” if it does not.
Poll count	Number of polls, in a row, given to this secondary at this time.
chain	Shows the previous (p) and next (n) secondary address on this interface in the round-robin loop of polled devices.

Sample show interfaces accounting Display

The following is sample output from the **show interfaces accounting** command:

```
Router# show interfaces accounting
Interface TokenRing0 is disabled
Ethernet0
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
                      IP     873171  735923409      34624    9644258
                  Novell     163849   12361626      57143    4272468
                 DEC MOP          0          0          1         77
                     ARP      69618    4177080       1529      91740
Interface Serial0 is disabled
Ethernet1
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
                      IP          0          0         37      11845
                  Novell          0          0       4591     275460
                 DEC MOP          0          0          1         77
                     ARP          0          0          7        420
Interface Serial1 is disabled
Interface Ethernet2 is disabled
Interface Serial2 is disabled
Interface Ethernet3 is disabled
Interface Serial3 is disabled
Interface Ethernet4 is disabled
Interface Ethernet5 is disabled
Interface Ethernet6 is disabled
Interface Ethernet7 is disabled
Interface Ethernet8 is disabled
Interface Ethernet9 is disabled
Fddi0
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
                  Novell          0          0        183      11163
                     ARP          1         49          0          0
```

When the output indicates that an interface is “ disabled,” the router has received excessive errors (over 5000 in a keepalive period).

Example with Flow-Based WRED

The following is sample output from the **show interfaces** command issued for the serial interface 1 for which flow-based WRED is enabled. The output shows that there are 8 active flow-based WRED flows, that the maximum number of flows active at any time is 9, and that the maximum number of possible flows configured for the interface is 16:

```
Router# show interfaces serial 1
Serial1 is up, line protocol is up
  Hardware is HD64570
  Internet address is 10.1.2.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
Reliability 255/255, txload 237/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive not set
  Last input 00:00:22, output 00:00:00, output hang never
  Last clearing of "show interface" counters 00:17:58
  Input queue: 0/75/0 (size/max/drops); Total output drops: 2479
Queueing strategy: random early detection(RED)
    flows (active/max active/max): 8/9/16
```

```
    mean queue depth: 27
    drops: class  random   tail     min-th   max-th   mark-prob
           0      946      0        20       40       1/10
           1      488      0        22       40       1/10
           2      429      0        24       40       1/10
           3      341      0        26       40       1/10
           4      235      0        28       40       1/10
           5      40       0        31       40       1/10
           6      0        0        33       40       1/10
           7      0        0        35       40       1/10
           rsvp   0        0        37       40       1/10
  30 second input rate 1000 bits/sec, 2 packets/sec
  30 second output rate 119000 bits/sec, 126 packets/sec
     1346 packets input, 83808 bytes, 0 no buffer
     Received 12 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     84543 packets output, 9977642 bytes, 0 underruns
     0 output errors, 0 collisions, 6 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Example with DWFQ

The following is sample output from the **show interfaces** command when distributed weighted fair queueing (DWFQ) is enabled on an interface. Notice that the queueing strategy is listed as “VIP-based fair queueing.”

```
Router# show interfaces fastethernet 1/1/0
Fast Ethernet 1/1/0 is up, line protocol is up
  Hardware is cyBus Fast Ethernet Interface, address is 0007.f618.4448 (bia 00e0)
  Description: pkt input i/f for WRL tests (to pagent)
  Internet address is 10.0.2.70/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive not set, fdx, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 01:11:01, output hang never
  Last clearing of "show interface" counters 01:12:31
  Queueing strategy: VIP-based fair queueing
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast
     0 input packets with dribble condition detected
     1 packets output, 60 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffers copied, 0 interrupts, 0 failures
```

Example with DNIS Binding

When the **show interfaces** command is issued on an unbound dialer interface, the output looks as follows:

```
Router# show interfaces dialer 0
Dialer0 is up (spoofing), line protocol is up (spoofing)
  Hardware is Unknown
  Internet address is 10.1.1.2/8
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 3/255
  Encapsulation PPP, loopback not set
  DTR is pulsed for 1 seconds on reset
  Last input 00:00:34, output never, output hang never
  Last clearing of "show interface" counters 00:05:09
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 1000 bits/sec, 0 packets/sec
     18 packets input, 2579 bytes
     14 packets output, 5328 bytes
```

But when the **show interfaces** command is issued on a bound dialer interface, you will get an additional report that indicates the binding relationship. The output is shown here:

```
Router# show interfaces dialer 0
Dialer0 is up, line protocol is up
  Hardware is Unknown
  Internet address is 10.1.1.2/8
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation PPP, loopback not set
  DTR is pulsed for 1 seconds on reset
  Interface is bound to BRI0:1
  Last input 00:00:38, output never, output hang never
  Last clearing of "show interface" counters 00:05:36
Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     38 packets input, 4659 bytes
     34 packets output, 9952 bytes
Bound to:
BRI0:1 is up, line protocol is up
  Hardware is BRI
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive not set
  Interface is bound to Dialer0 (Encapsulation PPP)
  LCP Open, multilink Open
  Last input 00:00:39, output 00:00:11, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     78 packets input, 9317 bytes, 0 no buffer
     Received 65 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     93 packets output, 9864 bytes, 0 underruns
     0 output errors, 0 collisions, 7 interface resets
     0 output buffer failures, 0 output buffers swapped out
     4 carrier transitions
```

At the end of the Dialer0 output, the **show interfaces** command is executed on each physical interface bound to it.

The following is sample output from the **show interfaces dialer stats** command:

```
Router# show interfaces dialer 0 stats
```

```
Dialer0
  Switching path    Pkts In   Chars In   Pkts Out  Chars Out
       Processor          0          0          6       1694
       Route cache  2522229  610372530     720458  174343542
             Total  2522229  610372530     720464  174345236
```

Example with BRI

In this example, the physical interface is the B1 channel of the BRI0 link. This example also illustrates that the output under the B channel keeps all hardware counts that are not displayed under any logical or virtual access interface. The line in the report that states "Interface is bound to Dialer0 (Encapsulation LAPB)" indicates that the B interface is bound to Dialer0 and the encapsulation running over this connection is Link Access Procedure, Balanced (LAPB), not PPP, which is the encapsulation configured on the D interface and inherited by the B channel.

```
Router# show interfaces bri0:1
BRI0:1 is up, line protocol is up
  Hardware is BRI
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive not set

Interface is bound to Dialer0 (Encapsulation LAPB)
  LCP Open, multilink Open
  Last input 00:00:31, output 00:00:03, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 1 packets/sec
  5 minute output rate 0 bits/sec, 1 packets/sec
     110 packets input, 13994 bytes, 0 no buffer
     Received 91 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     135 packets output, 14175 bytes, 0 underruns
     0 output errors, 0 collisions, 12 interface resets
     0 output buffer failures, 0 output buffers swapped out
     8 carrier transitions
```

Any protocol configuration and states should be displayed from the Dialer0 interface.

Example with a Fast Ethernet SPA on a Cisco 7304 Router

The following is sample output from the **show interfaces fastethernet** command for the second interface (port 1) in a 4-Port 10/100 Fast Ethernet SPA located in the bottom subslot (1) of the Modular Service Cards (MSC) that is installed in slot 2 on a Cisco 7304 router:

```
Router# show interfaces fastethernet 2/1/1
FastEthernet2/1/1 is up, line protocol is up
  Hardware is SPA-4FE-7304, address is 00b0.64ff.5d80 (bia 00b0.64ff.5d80)
  Internet address is 192.168.50.1/24
  MTU 9216 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:22, output 00:00:02, output hang never
  Last clearing of "show interface" counters never
```

```
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     5 packets input, 320 bytes
     Received 1 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     8 packets output, 529 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 babbles, 0 late collision, 0 deferred
     2 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Example for an Interface with an Asymmetric Receiver and Transmitter Rates

```
Router# show interfaces e4/0
Ethernet4/0 is up, line protocol is up
  Hardware is AmdP2, address is 000b.bf30.f470 (bia 000b.bf30.f470)
  Internet address is 10.1.1.9/24
  MTU 1500 bytes, BW 10000 Kbit, RxBW 5000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 254/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:01, output hang never
  Last clearing of "show interface" counters 00:03:36
  Input queue: 34/75/0/819 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  30 second input rate 7138000 bits/sec, 14870 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
     3109298 packets input, 186557880 bytes, 0 no buffer
     Received 217 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     22 packets output, 1320 bytes, 0 underruns
     11 output errors, 26 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

The table below describes the significant fields shown in the display.

Table 117: show interfaces fastethernet Field Descriptions--Fast Ethernet SPA

Field	Description
Fast Ethernet...is up ...is administratively down	Indicates whether the interface hardware is currently active and if it has been taken down by an administrator.
line protocol is	Indicates whether the software processes that handle the line protocol consider the line usable or if it has been taken down by an administrator.
Hardware	Hardware type (for example, SPA-4FE-7304) and MAC address.

Field	Description
Description	Alphanumeric string identifying the interface. This appears only if the **description** interface configuration command has been configured on the interface.
Internet address	Internet address followed by subnet mask.
MTU	Maximum transmission unit of the interface. The default is 1500 bytes for the 4-Port 10/100 Fast Ethernet SPA.
BW	Bandwidth of the interface in kilobits per second.
RxBW	Receiver bandwidth of the interface, in kilobits per second. This value is displayed only when an interface has asymmetric receiver and transmitter rates.
DLY	Delay of the interface in microseconds.
reliability	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
txload, rxload	Load on the interface (in the transmit "tx" and receive "rx" directions) as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method assigned to the interface.
loopback	Indicates whether loopback is set.
Keepalive	Indicates whether keepalives are set, and the time interval.
Half-duplex, Full-duplex	Indicates the duplex mode for the interface.
100Mb/s, 10Mb/s	Speed of the interface in megabits per second.
100BaseTX/FX	Media protocol standard.
ARP type:	Type of ARP assigned and the timeout period.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This field is not updated by fast-switched traffic.
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by the interface. Useful for knowing when a dead interface failed.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is displayed. If that field overflows, asterisks are printed. **Note** This field does not apply to SPA interfaces.

Field	Description
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. A series of asterisks (***) indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 231 ms (and less than 232 ms) ago.
Input queue (size/max/drops/flushes)	Packet statistics on the input queue reported as: • Size--Number of packets in the input queue. • Max--Maximum size of the queue. • Drops--Number of packets dropped because of a full input queue. • Flushes--Number of packets dropped as part of selective packet discard (SPD). SPD implements a selective packet drop policy on the router's IP process queue. Therefore, it applies only to process-switched traffic.
Total output drops	Total number of packets dropped because of a full output queue.
Queueing strategy	Type of Layer 3 queueing active on this interface. The default is first-in, first-out (FIFO).
Output queue (size/max)	Number of packets in the output queue (size), and the maximum size of the queue (max).
5 minute input rate, 5 minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic it sends and receives (rather than all network traffic). The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
Received...broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium. For instance, any Ethernet packet that is smaller than 64 bytes is considered a runt.

Field	Description
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium. For example, any Ethernet packet that is larger than 1536 bytes is considered a giant. **Note** For the 4-Port 10/100 Fast Ethernet SPA, the default is that a giant is any packet greater than 1536 bytes. However, if you modify the maximum transmission unit (MTU) for the interface, this counter increments when you exceed the specified MTU for the interface.
throttles	Number of times the receiver on the port was disabled, possibly because of buffer or processor overload.
input errors	Includes runts, giants, no buffer, cyclic redundancy check (CRC), frame, overrun, and ignored counts. Other input-related errors can also cause the input errors count to be increased, and some datagrams may have more than one error; therefore, this sum may not balance with the sum of enumerated input error counts.
CRC	Cyclic redundancy check generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a LAN, this is usually the result of collisions or a malfunctioning Ethernet device.
overrun	Number of times the receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers. Broadcast storms and bursts of noise can cause the ignored count to be increased.
watchdog	Number of times the watchdog receive timer expired. Expiration happens when receiving a packet with a length greater than 2048 bytes.
input packets with dribble condition detected	Dribble bit error indicates that a frame is slightly too long. This frame error counter is incremented for informational purposes only; the router accepts the frame.
packets output	Total number of messages transmitted by the system.
bytes	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the transmitter has been running faster than the router can handle.

Field	Description
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors, because some datagrams may have more than one error and others may have errors that do not fall into any of the specifically tabulated categories.
collisions	Number of messages retransmitted because of an Ethernet collision. This is usually the result of an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). A packet that collides is counted only once in output packets.
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within several seconds. Interface resets can occur when an interface is looped back or shut down.
babbles	Transmit jabber timer expired.
late collision	Number of late collisions. Late collision happens when a collision occurs after transmitting the preamble.
deferred	Number of times that the interface had to defer while ready to transmit a frame because the carrier was asserted.
lost carrier	Number of times the carrier was lost during transmission.
no carrier	Number of times the carrier was not present during the transmission. **Note** This field does not apply to SPA interfaces.
output buffer failures, output buffers swapped out	These counters are not used by the 4-Port 10/100 Fast Ethernet SPA on the Cisco 7304 router.

Example with a Gigabit Ethernet SPA on a Cisco 7304 Router

The following is sample output from the **show interfaces gigabitethernet** command for the first interface (port 0) in a 2-Port 10/100/1000 Gigabit Ethernet SPA located in the top subslot (0) of the MSC that is installed in slot 4 on a Cisco 7304 router:

```
Router# show interfaces gigabitethernet 4/0/0

GigabitEthernet4/0/0 is up, line protocol is down
  Hardware is SPA-2GE-7304, address is 00b0.64ff.5a80 (bia 00b0.64ff.5a80)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 1000Mb/s, link type is auto, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:09, output hang never
  Last clearing of "show interface" counters never
```

```
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     109 packets output, 6540 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 babbles, 0 late collision, 0 deferred
     1 lost carrier, 0 no carrier, 0 PAUSE output
     0 output buffer failures, 0 output buffers swapped out
```

Example with Gigabit Ethernet SPAs Configured as Primary and Backup Interfaces on a Cisco 7600 Router

The following examples show the additional lines included in the display when the command is issued on two Gigabit Ethernet interfaces that are configured as a primary interface (gi3/0/0) and as a backup interface (gi3/0/11) for the primary:

```
Router# show interfaces gigabitEthernet 3/0/0

GigabitEthernet3/0/0 is up, line protocol is up (connected)
  Hardware is GigEther SPA, address is 0005.dc57.8800 (bia 0005.dc57.8800)
  Backup interface GigabitEthernet3/0/11, failure delay 0 sec, secondary disable delay 0
sec,
  .
  .
  .
Router# show interfaces gigabitEthernet 3/0/11

GigabitEthernet3/0/11 is standby mode, line protocol is down (disabled)
  .
  .
  .
```

The table below describes the fields shown in the display for Gigabit Ethernet SPA interfaces.

Table 118: show interfaces gigabitethernet Field Descriptions--Gigabit Ethernet SPA

Field	Description
GigabitEthernet...is up ...is administratively down	Indicates whether the interface hardware is currently active and if it has been taken down by an administrator.
line protocol is	Indicates whether the software processes that handle the line protocol consider the line usable or if it has been taken down by an administrator.
Hardware	Hardware type (for example, SPA-2GE-7304) and MAC address.
Backup interface	Identifies the backup interface that exists for this, the primary interface.

Field	Description
Failure and secondary delay	The period of time (in seconds) to delay bringing up the backup interface when the primary goes down, and bringing down the backup after the primary becomes active again. On the Cisco 7600 router, the delay must be 0 (the default) to ensure that there is no delay between when the primary goes down and the backup comes up, and vice versa.
Standby mode	Indicates that this is a backup interface and that it is currently operating in standby mode.
Description	Alphanumeric string identifying the interface. This appears only if the **description** interface configuration command has been configured on the interface.
Internet address	Internet address followed by subnet mask.
MTU	Maximum transmission unit of the interface. The default is 1500 bytes for the 2-Port 10/100/1000 Gigabit Ethernet SPA.
BW	Bandwidth of the interface in kilobits per second.
DLY	Delay of the interface in microseconds.
reliability	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
txload, rxload	Load on the interface (in the transmit “tx” and receive “rx” directions) as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method assigned to the interface.
loopback	Indicates whether loopback is set.
Keepalive	Indicates whether keepalives are set, and the time interval.
Half-duplex, Full-duplex	Indicates the duplex mode for the interface.
1000Mb/s, 100Mb/s, 10Mb/s	Speed of the interface in megabits per second.
link type	Specifies whether autonegotiation is being used on the link.
media type	Interface port media type: RJ45, SX, LX, or ZX.
100BaseTX/FX	Media protocol standard.
ARP type:	Type of ARP assigned and the timeout period.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This field is not updated by fast-switched traffic.

Field	Description
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by the interface. Useful for knowing when a dead interface failed.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is displayed. If that field overflows, asterisks are printed. **Note** This field does not apply to SPA interfaces.
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. A series of asterisks (***) indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 231 ms (and less than 232 ms) ago.
Input queue (size/max/drops/flushes)	Packet statistics on the input queue reported as: • Size--Number of packets in the input queue. • Max--Maximum size of the queue. • Drops--Number of packets dropped because of a full input queue. • Flushes--Number of packets dropped as part of SPD. SPD implements a selective packet drop policy on the router's IP process queue. Therefore, it applies only to process-switched traffic.
Total output drops	Total number of packets dropped because of a full output queue.
Queueing strategy	Type of Layer 3 queueing active on this interface. The default is FIFO.
Output queue (size/max)	Number of packets in the output queue (size), and the maximum size of the queue (max).
5 minute input rate, 5 minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic it sends and receives (rather than all network traffic). The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.

Field	Description
Received...broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium. For instance, any Ethernet packet that is smaller than 64 bytes is considered a runt.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium. For example, any Ethernet packet that is larger than 1536 bytes is considered a giant. **Note** For the 2-Port 10/100/1000 Gigabit Ethernet SPA, the default is that a giant is any packet greater than 1536 bytes. However, if you modify the MTU for the interface, this counter increments when you exceed the specified MTU for the interface.
throttles	Number of times the receiver on the port was disabled, possibly because of buffer or processor overload.
input errors	Includes runts, giants, no buffer, CRC, frame, overrun, and ignored counts. Other input-related errors can also cause the input errors count to be increased, and some datagrams may have more than one error; therefore, this sum may not balance with the sum of enumerated input error counts.
CRC	Cyclic redundancy check generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a LAN, this is usually the result of collisions or a malfunctioning Ethernet device.
overrun	Number of times the receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers. Broadcast storms and bursts of noise can cause the ignored count to be increased.
watchdog	Number of times the watchdog receive timer expired. Expiration happens when receiving a packet with a length greater than 2048 bytes.
input packets with dribble condition detected	Dribble bit error indicates that a frame is slightly too long. This frame error counter is incremented for informational purposes only; the router accepts the frame.
packets output	Total number of messages transmitted by the system.

Field	Description
bytes	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the transmitter has been running faster than the router can handle.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors, because some datagrams may have more than one error and others may have errors that do not fall into any of the specifically tabulated categories.
collisions	Number of messages retransmitted because of an Ethernet collision. This is usually the result of an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). A packet that collides is counted only once in output packets.
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within several seconds. Interface resets can occur when an interface is looped back or shut down.
babbles	Transmit jabber timer expired.
late collision	Number of late collisions. Late collision happens when a collision occurs after transmitting the preamble.
deferred	Number of times that the interface had to defer while ready to transmit a frame because the carrier was asserted.
lost carrier	Number of times the carrier was lost during transmission.
no carrier	Number of times the carrier was not present during the transmission. **Note** This field does not apply to SPA interfaces.
output buffer failures, output buffers swapped out	These counters are not used by the 2-Port 10/100/1000 Gigabit Ethernet SPA on the Cisco 7304 router.

Example with a Packet over SONET/SDH (POS) SPA on a Cisco 7600 Series Router and Catalyst 6500 Series Switch

The following is sample output from the **show interfaces pos** command on a Cisco 7600 series router or Catalyst 6500 series switch for POS interface 4/3/0 (which is the interface for port 0 of the SPA in subslot 3 of the SIP in chassis slot 4):

```
Router# show interfaces pos 4/3/0

POS4/3/0 is up, line protocol is up  (APS working - active)
  Hardware is Packet over SONET
  Internet address is 10.0.0.1/8
```

```
MTU 4470 bytes, BW 622000 Kbit, DLY 100 usec, rely 255/255, load 1/255
Encapsulation HDLC, crc 16, loopback not set
Keepalive not set
Scramble disabled
Last input 00:00:34, output 04:09:06, output hang never
Last clearing of "show interface" counters never
Queueing strategy:fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
      Available Bandwidth 622000 kilobits/sec
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
   782 packets input, 226563 bytes, 0 no buffer
   Received 0 broadcasts, 1 runts, 0 giants, 0 throttles
            0 parity
   1 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
   271 packets output, 28140 bytes, 0 underruns
   0 output errors, 0 applique, 2 interface resets
   0 output buffer failures, 0 output buffers swapped out
   2 carrier transitions
```

The table below describes the significant fields shown in this display.

*Table 119: **show interfaces pos** Field Descriptions--POS SPA*

Field	Description
POS4/3/0 is up, line protocol is up	Indicates whether the interface hardware is currently active and can transmit and receive or whether it has been taken down by an administrator.
Hardware is. . .	Hardware type: • For POSIP--cyBus Packet over SONET • For POS SPAs--Packet over SONET
Internet address is	Internet address and subnet mask.
MTU	Maximum transmission unit of the interface.
BW	Bandwidth of the interface, in kilobits per second.
DLY	Delay of the interface, in microseconds.
rely	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes. The calculation uses the value from the **bandwidth** interface configuration command.
Encapsulation	Encapsulation method assigned to the interface.
Loopback	Indicates whether loopbacks are set.
Keepalive	Indicates whether keepalives are set.

Field	Description
Scramble	Indicates whether SONET payload scrambling is enabled. SONET scrambling is disabled by default. For the POS SPAs on the Cisco 12000 series routers, scrambling is enabled by default.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This counter is updated only when packets are process-switched, not when packets are fast-switched.
(Last) output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by an interface. This counter is updated only when packets are process-switched, not when packets are fast-switched.
(Last) output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. *** indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 2231 ms (and less than 232 ms) ago.
Queueing strategy	FIFO queueing strategy (other queueing strategies you might see are priority-list, custom-list, and weighted fair).
Output queue, drops input queue, drops	Number of packets in output and input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped because a queue was full.
5 minute input rate 5 minute output rate	Average number of bits and packets received or transmitted per second in the last 5 minutes.
packets input	Total number of error-free packets received by the system.
bytes (input)	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with number of packets ignored. Broadcast storms on Ethernets and bursts of noise on serial lines are often responsible for no input buffer events.
broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium.

Field	Description
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium.
throttles	Not supported for POS interfaces.
parity	Report of the parity errors on the interface.
input errors	Total number of no buffer, runts, giants, CRCs, frame, overrun, ignored, and abort counts. Other input-related errors can also increment the count, so that this sum might not balance with the other counts.
CRC	Cyclic redundancy checksum generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data. On a serial link, CRCs usually indicate noise, gain hits, or other transmission problems on the data link.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a serial line, this is usually the result of noise or other transmission problems.
overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be incremented.
abort	Illegal sequence of one bits on the interface.
packets output	Total number of messages transmitted by the system.
bytes (output)	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the far-end transmitter has been running faster than the near-end router's receiver can handle.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this might not balance with the sum of the enumerated output errors, because some datagrams can have more than one error, and others can have errors that do not fall into any of the specifically tabulated categories.
applique	Indicates an unrecoverable error has occurred on the POSIP applique. The system then invokes an interface reset.

Field	Description
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within a certain interval. If the system notices that the carrier detect line of an interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an unrecoverable interface processor error occurred, or when an interface is looped back or shut down.
output buffer failures	Not supported for POS interfaces.
output buffers swapped out	Not supported for POS interfaces.
carrier transitions	Number of times the carrier detect signal of the interface has changed state.

Example with a POS SPA on a Cisco 12000 Series Router

The following is sample output from the **show interfaces pos** command on a Cisco 12000 series router for POS interface 1/1/0 (which is the interface for port 0 of the SPA in subslot 1 of the SIP in chassis slot 1):

```
Router# show interfaces pos 1/1/0

POS1/1/0 is up, line protocol is up
  Hardware is Packet over SONET
  Internet address is 10.41.41.2/24
  MTU 4470 bytes, BW 9952000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation HDLC, crc 32, loopback not set
  Keepalive not set
  Scramble enabled
  Last input 00:00:59, output 00:00:11, output hang never
  Last clearing of "show interface" counters 00:00:14
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
        Available Bandwidth 9582482 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
              0 parity
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     1 packets output, 314 bytes, 0 underruns
     0 output errors, 0 applique, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
```

Example of Displaying Traffic for a Specific Interface on a Cisco CSR 1000v Series Cloud Services Router

For each interface on the router, the **show interfaces** command displays information about the link. In the following example, for the line starting with `Full Duplex`, the interface port media type is: `Virtual`, not a physical media type such as `RJ45`. This shows that the interface belongs to a cloud services router (Cisco CSR 1000v Series Cloud Services Router (CSR 1000v) or Cisco Integrated Services Router (ISRv)).

```
Router# show interfaces GigabitEthernet1

GigabitEthernet1 is up, line protocol is up
  Hardware is CSR vNIC, address is 000d.3a16.20f1 (bia 000d.3a16.20f1)
  Internet address is 12.0.0.4/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 1000Mbps, link type is auto, media type is Virtual
```

Example with a POS SPA SDCC Interface on a Cisco 12000 Series Router

The following is sample output from the **show interfaces sdcc**command on a Cisco 12000 series router for POS interface 1/1/0 (which is the interface for port 0 of the SPA in subslot 1 of the SIP in chassis slot 1):

```
Router# show interfaces sdcc 1/1/0

SDCC1/1/0 is administratively down, line protocol is down
  Hardware is SDCC
  MTU 1500 bytes, BW 192 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, crc 32, loopback not set
  Keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 00:01:55
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
```

The table below describes the significant fields shown in the display.

*Table 120: **show interfaces sdcc** Field Descriptions--POS SPA*

Field	Description
SDCC1/1/0 is administratively down, line protocol is down	Indicates whether the interface hardware is currently active and can transmit and receive or whether it has been taken down by an administrator.
Hardware is. . .	Hardware type is SDCC--Section Data Communications Channel.
Internet address is	Internet address and subnet mask.
MTU	Maximum transmission unit of the interface.

Field	Description
BW	Bandwidth of the interface, in kilobits per second.
DLY	Delay of the interface, in microseconds.
rely	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes. The calculation uses the value from the **bandwidth** interface configuration command.
Encapsulation	Encapsulation method assigned to the interface.
crc	Cyclic redundancy check size (16 or 32 bits).
Loopback	Indicates whether loopback is set.
Keepalive	Indicates whether keepalives are set.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This counter is updated only when packets are process-switched, not when packets are fast-switched.
(Last) output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by an interface. This counter is updated only when packets are process-switched, not when packets are fast-switched.
(Last) output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. *** indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 2231 ms (and less than 232 ms) ago.
Queueing strategy	FIFO queueing strategy (other queueing strategies you might see are priority-list, custom-list, and weighted fair).
Output queue, drops input queue, drops	Number of packets in output and input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped because a queue was full.
5 minute input rate 5 minute output rate	Average number of bits and packets received or transmitted per second in the last 5 minutes.

Field	Description
packets input	Total number of error-free packets received by the system.
bytes (input)	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with number of packets ignored. Broadcast storms on Ethernets and bursts of noise on serial lines are often responsible for no input buffer events.
broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium.
throttles	Not supported for POS interfaces.
parity	Report of the parity errors on the interface.
input errors	Total number of no buffer, runts, giants, CRCs, frame, overrun, ignored, and abort counts. Other input-related errors can also increment the count, so that this sum might not balance with the other counts.
CRC	Cyclic redundancy checksum generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data. On a serial link, CRCs usually indicate noise, gain hits, or other transmission problems on the data link.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a serial line, this is usually the result of noise or other transmission problems.
overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be incremented.
abort	Illegal sequence of one bits on the interface.
packets output	Total number of messages transmitted by the system.
bytes (output)	Total number of bytes, including data and MAC encapsulation, transmitted by the system.

Field	Description
underruns	Number of times that the far-end transmitter has been running faster than the near-end router's receiver can handle.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this might not balance with the sum of the enumerated output errors, because some datagrams can have more than one error, and others can have errors that do not fall into any of the specifically tabulated categories.
collisions	Not supported for POS interfaces.
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within a certain interval. If the system notices that the carrier detect line of an interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an unrecoverable interface processor error occurred, or when an interface is looped back or shut down.
output buffer failures	Not supported for POS interfaces.
output buffers swapped out	Not supported for POS interfaces.
carrier transitions	Number of times the carrier detect signal of the interface has changed state.

Example with a T3/E3 Shared Port Adapter

The following example shows the interface serial statistics on the first port of a T3/E3 SPA installed in subslot 0 of the SIP located in chassis slot 5:

```
Router# show interfaces serial 5/0/0
Serial5/0/0 is up, line protocol is up
  Hardware is SPA-4T3E3
  Internet address is 10.1.1.2/24
  MTU 4470 bytes, BW 44210 Kbit, DLY 200 usec,
     reliability 255/255, txload 234/255, rxload 234/255
  Encapsulation HDLC, crc 16, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:05, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 40685000 bits/sec, 115624 packets/sec
  5 minute output rate 40685000 bits/sec, 115627 packets/sec
     4653081241 packets input, 204735493724 bytes, 0 no buffer
     Received 4044 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
              0 parity
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     4652915555 packets output, 204728203520 bytes, 0 underruns
     0 output errors, 0 applique, 4 interface resets
     0 output buffer failures, 0 output buffers swapped out
 2 carrier transitions
```

The table below describes the fields shown in the **show interfaces serial** output for a T3/E3 SPA.

Note The fields appearing in the ouput will vary depending on card type, interface configuration, and the status of the interface.

Table 121: show interfaces serial Field Descriptions--T3/E3 SPA

Field	Description
Serial	Name of the serial interface.
line protocol is	If the line protocol is up, the local router has received keepalive packets from the remote router. If the line protocol is down, the local router has not received keepalive packets form the remote router.
Hardware is	Designates the specific hardware type of the interface.
Internet address is	The IP address of the interface.
MTU	The maximum packet size set for the interface.
BW	Bandwidth in kilobits per second.
DLY	Interface delay in microseconds.
reliability	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
txload	Transmit load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
rxload	Receive load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method.
crc	CRC size in bits.
loopback	Indicates whether loopback is set.
keepalive	Indicates whether keepalives are set.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This counter is updated only when packets are process-switched, not when packets are fast-switched.
Last output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by an interface. Useful for knowing when a dead interface failed. This counter is updated only when packets are process-switched, not when packets are fast-switched.

Field	Description
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.
Last clearing of show interface counters	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. *** indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 231 milliseconds (and less than 232 ms) ago.
Input queue	Packet statistics on the input queue reported as: • Size--Current size of the input queue. • Max--Maximum size of the input queue. • Drops--Packets dropped because the queue was full. • Flushes--Number of times that data on queue has been discarded.
Total output drops	Total number of dropped packets.
Queueing strategy	FIFO queueing strategy (other queueing strategies you might see are priority-list, custom-list, and weighted fair).
Output queue	Number of packets in the output queue (size), and the maximum size of the queue (max).
5-minute input rate	Average number of bits and packets received per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic it sends and receives (rather than all network traffic). The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.
5-minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic it sends and receives (rather than all network traffic). The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.

Example with a 1-Port 10-Gigabit Ethernet SPA on a Cisco 12000 Series Router

The following is sample output from the **show interfaces tengigabitethernet** command for the only interface (port 0) in a 1-Port 10 Gigabit Ethernet SPA located in the top subslot (0) of the carrier card that is installed in slot 7 on a Cisco 12000 series router:

```
Router# show interfaces tengigabitethernet 7/0/0
TenGigabitEthernet7/0/0 is up, line protocol is up (connected)
  Hardware is TenGigEther SPA, address is 0000.0c00.0102 (bia 000f.342f.c340)
  Internet address is 10.1.1.2/24
  MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full-duplex, 10Gb/s
  input flow-control is on, output flow-control is on
ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:10, output hang never
  Last clearing of "show interface" counters 20:24:30
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  L2 Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes
  L3 in Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes mcast
  L3 out Switched: ucast: 0 pkt, 0 bytes mcast: 0 pkt, 0 bytes
     237450882 packets input, 15340005588 bytes, 0 no buffer
     Received 25 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     1676 packets output, 198290 bytes, 0 underruns
     0 output errors, 0 collisions, 4 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 PAUSE output
     0 output buffer failures, 0 output buffers swapped out
```

The table below describes the significant fields shown in the display.

Table 122: show interfaces tengigabitethernet Field Descriptions--10-Gigabit Ethernet SPA

Field	Description
TenGigabitEthernet...is up ...is administratively down	Indicates whether the interface hardware is currently active and if it has been taken down by an administrator.
line protocol is	Indicates whether the software processes that handle the line protocol consider the line usable or if it has been taken down by an administrator.
Hardware	Hardware type and MAC address.
Description	Alphanumeric string identifying the interface. This appears only if the **description** interface configuration command has been configured on the interface.
Internet address	Internet address followed by subnet mask.

Field	Description
MTU	Maximum transmission unit of the interface.
BW	Bandwidth of the interface in kilobits per second.
DLY	Delay of the interface in microseconds.
reliability	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
txload, rxload	Load on the interface (in the transmit "tx" and receive "rx" directions) as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method assigned to the interface.
loopback	Indicates whether loopback is set.
Keepalive	Indicates whether keepalives are set, and the time interval.
Half-duplex, Full-duplex	Indicates the duplex mode for the interface.
10Gb/s	Speed of the interface in Gigabits per second.
input flow control ...	Specifies if input flow control is on or off.
ARP type:	Type of ARP assigned and the timeout period.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This field is not updated by fast-switched traffic.
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by the interface. Useful for knowing when a dead interface failed.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is displayed. If that field overflows, asterisks are printed.
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. A series of asterisks (***) indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 231 ms (and less than 232 ms) ago.

Field	Description
Input queue (size/max/drops/flushes)	Packet statistics on the input queue reported as: • Size--Number of packets in the input queue. • Max--Maximum size of the queue. • Drops--Number of packets dropped because of a full input queue. • Flushes--Number of packets dropped as part of SPD. SPD implements a selective packet drop policy on the router's IP process queue. Therefore, it applies only to process-switched traffic.
Total output drops	Total number of packets dropped because of a full output queue.
Queueing strategy	Type of Layer 3 queueing active on this interface. The default is FIFO.
Output queue (size/max)	Number of packets in the output queue (size), and the maximum size of the queue (max).
5 minute input rate, 5 minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic it sends and receives (rather than all network traffic). The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.
L2 Switched	Provides statistics about Layer 2 switched traffic, including unicast and multicast traffic.
L3 in Switched	Provides statistics about received Layer 3 traffic.
L3 out Switched	Provides statistics about sent Layer 3 traffic.
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
Received...broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium.
throttles	Number of times the receiver on the port was disabled, possibly because of buffer or processor overload.

Field	Description
input errors	Includes runts, giants, no buffer, CRC, frame, overrun, and ignored counts. Other input-related errors can also cause the input errors count to be increased, and some datagrams may have more than one error; therefore, this sum may not balance with the sum of enumerated input error counts.
CRC	Cyclic redundancy check generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a LAN, this is usually the result of collisions or a malfunctioning Ethernet device.
overrun	Number of times the receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers. Broadcast storms and bursts of noise can cause the ignored count to be increased.
watchdog	Number of times the watchdog receive timer expired.
multicast	Number of multicast packets.
pause input	Number of pause packets received.
input packets with dribble condition detected	Dribble bit error indicates that a frame is slightly too long. This frame error counter is incremented for informational purposes only; the router accepts the frame.
packets output	Total number of messages transmitted by the system.
bytes	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the transmitter has been running faster than the router can handle.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors, because some datagrams may have more than one error and others may have errors that do not fall into any of the specifically tabulated categories.
collisions	Number of messages retransmitted because of an Ethernet collision. This is usually the result of an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). A packet that collides is counted only once in output packets.

Field	Description
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within several seconds. Interface resets can occur when an interface is looped back or shut down.
babbles	Transmit jabber timer expired.
late collision	Number of late collisions. Late collision happens when a collision occurs after transmitting the preamble.
deferred	Number of times that the interface had to defer while ready to transmit a frame because the carrier was asserted.
lost carrier	Number of times the carrier was lost during transmission.
no carrier	Number of times the carrier was not present during the transmission.
pause output	Number of pause packets transmitted.
output buffer failures, output buffers swapped out	Number of output butters failures and output buffers swapped out.

Displaying Traffic for a Specific Interface Example

This example shows how to display traffic for a specific interface:

```
Router# show interfaces GigabitEthernet1/1

GigabitEthernet0/1 is up, line protocol is up
  Hardware is BCM1125 Internal MAC, address is 0016.9de5.d9d1 (bia 0016.9de5.d9d1)
  Internet address is 172.16.165.40/27
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is RJ45
  output flow-control is XON, input flow-control is XON
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:11, output 00:00:08, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     10 packets input, 2537 bytes, 0 no buffer
     Received 10 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 46 multicast, 0 pause input
     0 input packets with dribble condition detected
     18 packets output, 3412 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     7 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     2 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

Note The unknown protocol drops field displayed in the above example refers to the total number of packets dropped due to unknown or unsupported types of protocol. This field occurs on several platforms such as the Cisco 3725, 3745, 3825, and 7507 series routers.

This example shows how to display traffic for a FlexWAN module:

```
Router# show interfaces pos 6/1/0.1

POS6/1/0.1 is up, line protocol is up
  Hardware is Packet over Sonet
  Internet address is 10.1.2.2/24
  MTU 4470 bytes, BW 155000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY <<<+++ no packets info after this line
Arches#sh mod 6
Mod Ports Card Type                              Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
  6    0  2 port adapter FlexWAN                 WS-X6182-2PA       SAD04340JY3
Mod MAC addresses                       Hw    Fw           Sw           Status
--- ---------------------------------- ------ ------------ ------------ -------
  6  0001.6412.a234 to 0001.6412.a273   1.3   12.2(2004022 12.2(2004022 Ok
Mod Online Diag Status
--- -------------------
  6 Pass
Router#
```

Related Commands

Command	Description
fair-queue	Enables WFQ.
interface	Configures an interface type and enters interface configuration mode.
show controllers fastethernet	Displays Fast Ethernet interface information, transmission statistics and errors, and applicable MAC destination address and VLAN filtering tables.
show controllers gigabitethernet	Displays Gigabit Ethernet interface information, transmission statistics and errors, and applicable MAC destination address and VLAN filtering tables.
show controllers pos	Displays information about the POS controllers.
show controllers serial	Displays controller statistics.

show interfaces accounting

To display the number of packets of each protocol type that have been sent through all configured interfaces, use the **showinterfacesaccounting** command in user EXEC or privileged EXEC mode.

show interfaces [{*interface type number* | **null** *interface-number* | **vlan** *vlan-id*}] **accounting**

Syntax Description

interface	(Optional) Interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **pos**, and **port-channel**, **atm**, and **ge-wan**.
type number	(Optional) Module and port number; see the "Usage Guidelines" section for valid values.
null *interface-number*	(Optional) Specifies the null interface; the valid value is **0**.
vlan *vlan-id*	(Optional) Specifies the VLAN ID; valid values are from 1 to 4094.

Command Modes

User EXEC

Privileged EXEC (#)

Command History

Release	Modification
12.2(17a)SX1	This command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRC	Support for IPv6 was added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.4(2)S	This command was integrated into Cisco IOS Release 15.4(2)S.

Usage Guidelines

Note The Pkts Out and Chars Out fields display IPv6 packet counts only. The Pkts In and Chars In fields display both IPv4 and IPv6 packet counts, except for tunnel interfaces. For tunnel interfaces, the IPv6 input packets are counted as IPv6 packets only.

Due to hardware limitations on the ASIC, PFC IPv4 and IPv6 packets cannot be differentiated in the Pkts In and Chars In fields for IP count the IPv6 and IPv4 packets that are hardware forwarded. The Pkts In and Chars In fields for IPv6 only count software-forwarded packets. The IP Pkts Out and Chars Out fields show IPv4 packets, and the IPv6 Pkts Out and Chars Out fields show IPv6 packets.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

The port channels from 257 to 282 are internally allocated and are supported on the CSM and the FWSM only.

If you do not enter any keywords, all counters for all modules are displayed.

Examples

This example shows how to display the number of packets of each protocol type that have been sent through all configured interfaces:

```
Device# show interfaces gigabitethernet 5/2 accounting

GigabitEthernet5/2
Protocol Pkts In Chars In Pkts Out Chars Out
IP       50521   50521000 0        0
DEC MOP  0       0        1        129
CDP      0       0        1        592
IPv6     11      834      96       131658
```

The table below describes the significant fields shown in the display.

Table 123: show interfaces accounting Command Output Fields

Field	Description
Protocol	Protocol that is operating on the interface.
Pkts In	For IP it is the number of IPv4 software switched, IPv4 and IPv6 hardware switched packets received for the specified protocol. For IPv6 it is the number of IPv6 software switched packets received for the specified protocol.
Chars In	For IP it is the number of IPv4 software switched, IPv4 and IPv6 hardware switched characters received for the specified protocol. For IPv6 it is the number of IPv6 software switched characters received for the specified protocol.
Pkts Out	For IP it is the number of IPv4 sofware and hardware switched packets transmitted for the specified protocol. For IPv6 it is the number of IPv6 sofware and hardware switched packets transmitted for the specified protocol.
Chars Out	For IP it is the number of IPv4 software and hardware switched characters transmitted for the specified protocol. For IPv6 it is the number of IPv6 software and hardware switched characters transmitted for the specified protocol.

Related Commands

Command	Description
show interfaces	Displays the status and statistics for the interfaces in the chassis.

show interfaces analysis-module

To display status, traffic data, and configuration information about the analysis module interface, use the **showinterfacesanalysis-module** command in user EXEC or privileged EXEC mode.

show interfaces analysis-module *slot/unit*

Syntax Description

slot	Number of the router chassis slot for the network module.
/ *unit*	Number of the daughter card on the network analysis module (NAM). For NAM, always use 0.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.3(4)XD	This command was introduced on the following platforms: Cisco 2600XM series, Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.3(8)T4	This command was implemented on the following platforms: Cisco 2811, Cisco 2821, and Cisco 2851.
12.3(11)T	This command was implemented on the Cisco 3800 series.

Usage Guidelines

The analysis module interface is a Fast Ethernet interface on the router that connects to the internal interface on the Network Analysis Module (NM-NAM).

Examples

The command in the following example displays status, traffic data, and configuration information about the analysis module interface when the NM-NAM is installed in slot 2 of a Cisco 3745.

```
Router# show interfaces analysis-module 2/0

Network-Analyzer2/0 is up, line protocol is up
  Hardware is I82559FE, address is 0001.a535.0920 (bia 0001.a535.0920)
  Internet address is 10.1.1.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:26, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 4682
  Queueing strategy: fifo
  Output queue: 0/60 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 36000 bits/sec, 22 packets/sec
     905 packets input, 38190 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     671863 packets output, 96101624 bytes, 0 underruns
```

```
0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

The table below describes the significant fields shown in the display.

Table 124: show interfaces analysis-module Field Descriptions

Field	Description
Network-Analyzer	Indicates whether the analysis module interface hardware is currently active. The analysis module interface is the router-side interface for the internal Ethernet segment between the router and the NAM network module. If the analysis module interface hardware is operational, the output states that the “Network-Analyzer 1/0 is up.” If the interface has been taken down by an administrator, the output states that the “Network-Analyzer 1/0 is administratively down.”
line protocol is	Indicates whether the software processes that handle the line protocol consider the line usable or whether the line has been taken down by an administrator.
Hardware is...address is	Hardware type and address.
MTU	Maximum transmission unit (MTU) of the analysis module interface.
BW	Bandwidth of the interface, in kbps.
DLY	Delay of the interface, in microseconds.
reliability	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
txload	Transmit load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
rxload	Receive load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method assigned to the interface.
loopback	Indicates whether or not loopback is set.
Keepalive	Indicates whether or not keepalives are set and the interval between keepalives if they have been set.
ARP type...ARP Timeout	Type of Address Resolution Protocol (ARP) assigned and length of timeout.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by the interface and processed locally on the router. This field is useful for detecting when a dead interface failed. **Note** This field is not updated by fast-switched traffic.

Field	Description
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by the interface. This field is useful for detecting when a dead interface failed.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because a transmission took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. Asterisks (***) indicate that the elapsed time is too large to be displayed.
Input queue	Number of packets in the input queue. Each number is followed by a slash, the maximum size of the queue, the number of packets dropped because of a full queue, and the number of times that queued packets have been discarded.
Total output drops	Number of packets in the output queue that have been dropped because of a full queue.
Queueing strategy	Queueing strategy applied to the interface, which is configurable under the interface. The default is FIFO (first-in, first-out).
Output queue	Number of packets in the output queue, and the maximum size of the queue. Each number is followed by a slash.
5 minute input rate, 5 minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic that it sends and receives (rather than all network traffic). The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within 2 percent of the instantaneous rate of a uniform stream of traffic over that period. **Note** The 5-minute period referenced in this output is a load interval that is configurable under the interface. The default value is 5 minutes.
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernets and bursts of noise on serial lines are often responsible for no input buffer events.
Received...broadcasts	Number of broadcasts received.

Field	Description
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium. For instance, any Ethernet packet that is less than 64 bytes is considered a runt.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium. For example, any Ethernet packet that is greater than 1518 bytes is considered a giant.
throttles	Number of times that the interface requested another interface within the router to slow down.
input errors	Errors that include runts, giants, no buffer, cyclic redundancy checksum (CRC), frame, overrun, and ignored counts. Other input-related errors can also cause the input errors count to be increased, and some datagrams may have more than one error; therefore, this sum may not balance with the sum of enumerated input error counts.
CRC	Errors created when the CRC generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station that is transmitting bad data.
frame	Number of packets received incorrectly that have a CRC error and a noninteger number of octets. On a LAN, this is usually the result of collisions or a malfunctioning Ethernet device.
overrun	Number of times that the receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets that were ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different from system buffer space described. Broadcast storms and bursts of noise can cause the ignored count to increase.
input packets with dribble condition detected	Number of packets with dribble condition. Dribble bit error indicates that a frame is slightly too long. This frame error counter is incremented just for informational purposes; the router accepts the frame.
packets output	Total number of messages that have been transmitted by the system.
bytes	Total number of bytes, including data and MAC encapsulation, that have been transmitted by the system.
underruns	Number of times that the transmitter has run faster than the router could handle. This may never be reported on some interfaces.

Field	Description
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface that is being examined. Note that this may not balance with the sum of the enumerated output errors, because some datagrams may have more than one error, and others may have errors that do not fall into any of the specifically tabulated categories.
collisions	Number of messages that have been retransmitted because of an Ethernet collision. This is usually the result of an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). A packet that collides is counted only once in output packets.
interface resets	Number of times an interface has been completely reset. This can happen if packets that were queued for transmission were not sent within several seconds. On a serial line, this can be caused by a malfunctioning modem that is not supplying the transmit clock signal or by a cable problem. If the system notices that the carrier detect line of a serial interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an interface is looped back or shut down.
babbles	Count of frames greater than 1518 bytes that have been transmitted, indicating that the transmitter has been on the interface longer than the time necessary to transmit the largest frame.
late collision	Number of late collisions. A collision becomes a late collision when it occurs after the preamble has been transmitted.
deferred	Deferred indicates that the chip, while ready to transmit a frame, had to defer because the carrier was asserted.
lost carrier	Number of times that the carrier was lost during transmission.
no carrier	Number of times that the carrier was not present during the transmission.
output buffer failures, output buffers swapped out	Number of failed buffers and number of buffers swapped out.

Related Commands

Command	Description
show controllers analysis-module	Displays controller information for the analysis module interface.

show interfaces bdi

To display statistics for bridge domain interfaces (BDI) configured on the router, use the **show interfaces** command in privileged EXEC mode.

show interfaces [*type number*]

Syntax Description

number	(Optional) Port number on the selected interface.
accounting	(Optional) Displays the number of packets of each protocol type that have been sent through the interface.
controller	(Optional) Displays the interface status, configuration and controller status.
counters	(Optional) Displays the current status of the protocol counters enabled.
crb	(Optional) Displays interface routing or bridging information.
dampening	(Optional) Displays interface dampening information.
description	(Optional) Displays the interface description.
etherchannel	(Optional) Displays interface Ether Channel information.
history	(Optional) Displays the interface history.
irb	(Optional) Displays interface routing or bridging information.
mac-accounting	(Optional) Displays interface MAC accounting information.
mpls-exp	(Optional) Displays interface Multiprotocol Label Switching (MPLS) experimental accounting information.
precedence	(Optional) Displays interface precedence accounting information.
random-detect	(Optional) Displays interface Weighted Random Early Detection (WRED) information.
rate-limit	(Optional) Displays interface rate-limit information.
stats	(Optional) Displays interface packets and octets, in and out, by using switching path.
summary	(Optional) Displays an interface summary.

Command Default

This command has no default settings.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced on Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following example shows BDI configuration output:

```
Router# show interfaces BDI3
asr2#sh int bdi3
BDI3 is up, line protocol is up
Hardware is BDI, address is cafe.aaaa.0003 (bia 0024.14ab.86bf)
Internet address is 197.1.3.12/24
MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
reliability 255/255, txload 8/255, rxload 8/255
Encapsulation QinQ VLAN, outer ID  1, inner ID 2, loopback not set
Keepalive not supported
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:19:15, output 00:03:59, output hang never
Last clearing of "show interface" counters 00:17:36
Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 32947000 bits/sec, 73545 packets/sec
5 minute output rate 32877000 bits/sec, 73391 packets/sec
78126222 packets input, 4375068432 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
78126268 packets output, 4375071092 bytes, 0 underruns
0 output errors, 0 interface resets
0 unknown protocol drops
.
.
```

The following example shows the BDI interface summary:

```
Router#show interfaces bdi 3 summary
 *: interface is up
 IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
 RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
 TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
 TRTL: throttle count
  Interface                  IHQ       IQD       OHQ       OQD      RXBS      L
--------------------------------------------------------------------------------
  BDI3                         0         0         0         0         0      0
```

show interfaces capabilities

To display the interface capabilities for a module, an interface, or all interfaces, use the **showinterfacescapabilities** command in user EXEC or privileged EXEC mode.

show interfaces [*interface interface-number*] **capabilities** [**module** *number*]

Syntax Description

interface	(Optional) Interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **pos**, **atm**, and **port-channel**, and **ge-wan**.
interface-number	Module and port number; see the "Usage Guidelines" section for valid values.
module *number*	(Optional) Specifies the module number; see the "Usage Guidelines" section for valid values.

Command Default

This command has no default settings.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXE	This output was changed to include information about the following on the Supervisor Engine 720 only: • Port security • dot1x
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **pos**, **atm**, and **ge-wan** keywords are supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2

The *interface-number*argument designates the module and port number. Valid values for *interface-number* depend on the chassis and module that are used. For example, if you have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the slot number are from 2 to 13 and valid values for the port number are from 1 to 48.

The **port-channel** values are from 0 to 282; values from 257 to 282 are supported on the CSM and the FWSM only.

Examples

This example shows how to display the interface capabilities for a module:

```
Router> show interfaces capabilities module 6
FastEthernet6/1
Dot1x: yes
Model: WS-X6248-RJ-45
```

```
Type: 10/100BaseTX
Speed: 10,100,auto
Duplex: half,full
Trunk encap. type: 802.1Q,ISL
Trunk mode: on,off,desirable,nonegotiate
Channel: yes
Broadcast suppression: percentage(0-100)
Flowcontrol: rx-(off,on),tx-(none)
Membership: static
Fast Start: yes
QOS scheduling: rx-(1q4t), tx-(2q2t)
CoS rewrite: yes
ToS rewrite: yes
Inline power: no
SPAN: source/destination
UDLD yes
Link Debounce: yes
Link Debounce Time: no
Ports on ASIC: 1-12
Port-Security: yes
Router#
```

This example shows how to display the interface capabilities for an interface:

```
Router? show interfaces fastethernet 4/1 capabilities
FastEthernet4/1
Model: WS-X6348-RJ-45
Type: 10/100BaseTX
Speed: 10,100,auto
Duplex: half,full
Trunk encap. type: 802.1Q,ISL
Trunk mode: on,off,desirable,nonegotiate
Channel: yes
Broadcast suppression: percentage(0-100)
Flowcontrol: rx-(off,on),tx-(none)
Fast Start: yes
QOS scheduling: rx-(1q4t), tx-(2q2t)
CoS rewrite: yes
ToS rewrite: yes
Inline power: no
SPAN: source/destination
```

This example shows how to display the port-channel interface capabilities:

```
Router> show interfaces port-channel 12 capabilities
Port-channel12
  Model:                 NO IDPROM
  Type:                  unknown
  Speed:                 10,100,1000,auto
  Duplex:                half,full
  Trunk encap. type:     802.1Q,ISL
  Trunk mode:            on,off,desirable,nonegotiate
  Channel:               yes
  Broadcast suppression: percentage(0-100)
  Flowcontrol:           rx-(off,on),tx-(none)
  Fast Start:            yes
  QOS scheduling:        rx-(1q4t), tx-(1q4t)
  CoS rewrite:           yes
  ToS rewrite:           yes
  Inline power:          no
  SPAN:                  source/destination
```

Router#

Related Commands

Command	Description
show interfaces	Displays the status and statistics for the interfaces in the chassis.

show interfaces content-engine

To display basic interface configuration information for a content engine (CE) network module, use the **showinterfacescontent-engine** command in privileged EXEC mode.

show interfaces content-engine *slot/unit*

Syntax Description

slot	Number of the router chassis slot for the network module.
unit	Number of the daughter card on the network module. For CE network modules, always use 0.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)YT	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

The output for this command contains the basic configuration for the interface, as well as the number of packets transmitted, output rate, and so forth.

Examples

The following example displays interface status and data for the CE network module in slot 1 for Cisco 2600 series routers (except the Cisco 2691). Note that the bandwidth is 10 Mbps.

```
Router# show interfaces content-engine 1/0
Content-Engine1/0 is up, line protocol is up
  Hardware is I82559FE, address is 0006.280e.10b0 (bia 0006.280e.10b0)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:50, output 00:00:04, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     13 packets input, 5835 bytes, 0 no buffer
     Received 13 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     71 packets output, 6285 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

The following example displays interface status and data for a CE network module in slot 3 of a Cisco 2691. This example shows the 100-Mbps bandwidth of a Cisco 2691 and all the other supported routers except the remainder of the Cisco 2600 series.

```
Router# show interfaces content-engine 3/0
Content-Engine3/0 is up, line protocol is up
  Hardware is I82559FE, address is 0004.9a0b.4b30 (bia 0004.9a0b.4b30)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:41, output 00:00:04, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     14 packets input, 6176 bytes, 0 no buffer
     Received 14 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     109 packets output, 16881 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

The table below describes the significant fields shown in the display.

Table 125: show interfaces content-engine Field Descriptions

Field	Description
Content-Engine	Indicates whether the CE interface hardware is currently active. If the CE interface hardware is operational, the output states that "Content-Engine slot/port is up." If it has been taken down by an administrator, the output states that "Content-Engine slot/port is administratively down."
line protocol	Indicates whether the software processes that handle the line protocol consider the line usable or whether the line has been taken down by an administrator.
Hardware...address	Hardware type and address.
MTU	Maximum transmission unit (MTU) of the content engine interface.
BW	Bandwidth of the interface, in kilobits per second.
DLY	Delay of the interface, in microseconds.
reliability	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
txload	Transmit load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
rxload	Receive load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method assigned to the interface.

Field	Description
loopback	Indicates whether loopback is set.
Keepalive	Indicates whether keepalives are set and the interval between keepalives if they have been set.
ARP type...Timeout	Type of Address Resolution Protocol (ARP) assigned and length of timeout.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by the interface and processed locally on the router. This field is useful for detecting when a dead interface failed. **Note** This field is not updated by fast-switched traffic.
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by the interface. This field is useful for detecting when a dead interface failed.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because a transmission took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. Asterisks (***) indicate that the elapsed time is too large to be displayed. A time of all zeroes (0:00:00) indicates that the counters were cleared more than 231 ms (and less than 232 ms) ago.
Input queue	Number of packets in the input queue. Each number is followed by a slash, the maximum size of the queue, the number of packets dropped because of a full queue, and the number of times that queued packets have been discarded.
Total output drops	Number of packets in the output queue that have been dropped because of a full queue.
Queueing strategy	Queueing strategy applied to the interface, which is configurable under the interface. The default is FIFO.
Output queue	Number of packets in the output queue. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped because of a full queue.

Field	Description
5 minute input rate, 5 minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic that it sends and receives (rather than all network traffic). The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within 2 percent of the instantaneous rate of a uniform stream of traffic over that period. **Note** The 5-minute period referenced in this output is a load interval that is configurable under the interface. The default value is 5 minutes.
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernets and bursts of noise on serial lines are often responsible for no input buffer events.
Received...broadcasts	Number of broadcasts received.
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium. For instance, any Ethernet packet that is less than 64 bytes is considered a runt.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium. For example, any Ethernet packet that is greater than 1518 bytes is considered a giant.
throttles	Number of times that the interface requested another interface within the router to slow down.
input errors	Errors that include runts, giants, no buffer, cyclic redundancy check (CRC), frame, overrun, and ignored counts. Other input-related errors can also cause the input errors count to be increased, and some datagrams may have more than one error; therefore, this sum may not balance with the sum of enumerated input error counts.
CRC	Errors created when the CRC generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station that is transmitting bad data.
frame	Number of packets received incorrectly that have a CRC error and a non integer number of octets. On a LAN, this is usually the result of collisions or a malfunctioning Ethernet device.

Field	Description
overrun	Number of times that the receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets that were ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different from system buffer space described. Broadcast storms and bursts of noise can cause the ignored count to increase.
input packets with dribble condition detected	Number of packets with dribble condition. Dribble bit error indicates that a frame is slightly too long. This frame error counter is incremented just for informational purposes; the router accepts the frame.
packets output	Total number of messages that have been transmitted by the system.
bytes	Total number of bytes, including data and MAC encapsulation, that have been transmitted by the system.
underruns	Number of times that the transmitter has run faster than the router could handle. This may never be reported on some interfaces.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the content engine that is being examined. Note that this may not balance with the sum of the enumerated output errors, because some datagrams may have more than one error, and others may have errors that do not fall into any of the specifically tabulated categories.
collisions	Number of messages that have been retransmitted because of an Ethernet collision. This is usually the result of an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). A packet that collides is counted only once in output packets.
interface resets	Number of times an interface has been completely reset. This can happen if packets that were queued for transmission were not sent within several seconds. On a serial line, this can be caused by a malfunctioning modem that is not supplying the transmit clock signal or by a cable problem. If the system notices that the carrier detect line of a serial interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an interface is looped back or shut down.
babbles	Count of frames greater than 1518 bytes that have been transmitted, indicating that the transmitter has been on the interface longer than the time necessary to transmit the largest frame.
late collision	Number of late collisions. A collision becomes a late collision when it occurs after the preamble has been transmitted.
deferred	Deferred indicates that the chip, while ready to transmit a frame, had to defer because the carrier was asserted.
lost carrier	Number of times that the carrier was lost during transmission.

Field	Description
no carrier	Number of times that the carrier was not present during the transmission.
output buffer failures, output buffers swapped out	Number of failed buffers and number of buffers swapped out.

Related Commands

Command	Description
interface content-engine	Configures an interface for a CE network module and enters interface configuration mode.
show controllers content-engine	Displays controller information for CE network modules.

show interfaces counters nonzero

To get the counter information for ports which have non zero values, use the **showinterfacescountersnonzero** command in user EXEC or privileged EXEC mode.

show interfaces counters nonzero [**module** *number*]

Syntax Description

module	(Optional) Limits display to interfaces on module.
number	The module number has a range from 1 to 6.

Command Default

This command has no default settings.

Command Modes

EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(18)SXF	This command was introduced for Cisco IOS Release 12.2(18)SXF.
12.2(32)SX	This command was integrated into Cisco IOS Release 12.2(32)SX.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(32)XJC	This command was integrated into Cisco IOS Release 12.2(32)XJC.

Usage Guidelines

Use the **showinterfacescountersnonzero** command to get the counter information for ports which have non zero values.

Examples

The following example shows the output of **showinterfacescountersnonzero** command. The output is displayed only if any one of the counters is non zero. The counters are checked for all the ports present in the router.

```
Router#sh interfaces counters nonzero
Port               InOctets   InUcastPkts   InMcastPkts   InBcastPkts
Fa3/1             110519159        253605       1276951           574
Gi6/2             120329657        213823       1294339         67009
Port              OutOctets  OutUcastPkts  OutMcastPkts  OutBcastPkts
Fa3/1              15950485           142         41048             1
Gi6/2              15475538           431         41036             6
Port     Last-Clear-Counters
Gi1/1         never
Gi1/2         never
Gi1/3         never
Gi1/4         never
Gi1/5         never
Gi1/6         never
Gi1/7         never
Gi1/8         never
Fa3/1         never
Fa3/2         never
Fa3/3         never
```

```
Fa3/4         never
Router#
```

Related Commands

Command	Description
show interfaces counters	Displays the traffic seen by the physical interface.

show interfaces ctunnel

To display information about an IP over Connectionless Network service (CLNS) tunnel (CTunnel), use the **showinterfacesctunnel** command in privileged EXEC mode.

show interfaces ctunnel *interface-number* [**accounting**]

Syntax Description

interface-number	Virtual interface number.
accounting	(Optional) Displays the number of packets of each protocol type that have been sent through the interface.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

For the **showinterfacesctunnel** command, all output that relates to a physical medium is irrelevant and should be ignored because the CTunnel is a virtual interface.

Examples

The following is sample output from the **showinterfacesctunnel** command:

```
Router# show interfaces ctunnel 1
CTunnel1 is up, line protocol is up
  Hardware is CTunnel
  Internet address is 10.0.0.1/24
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
      reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive set (10 sec)
  Tunnel destination 49.0001.2222.2222.2222.cc
  Last input never, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/0, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     1 packets output, 104 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

The table below describes the significant fields shown in the display.

*Table 126: **show interfaces ctunnel** Field Descriptions*

Field	Description
CTunnel is {up | down | administratively down}	Interface is currently active (up) or inactive (down). Shows interface is administratively down if disabled.
line protocol is {up | down}	Shows line protocol up if a valid route is available to the CLNS tunnel (CTunnel) destination. Shows line protocol down if no route is available, or if the route would be recursive.
Hardware	Type of interface, in this instance CTunnel.
Internet address	IP address of the interface.
MTU	Maximum transmission unit of the interface.
BW	Bandwidth, as specified by the user, that is available on the link.
DLY	Delay of the interface, in microseconds.
Encapsulation	Encapsulation method is always TUNNEL for tunnels.
Loopback	Shows whether loopback is set or not.
Keepalive	Shows whether keepalives are set or not.
Tunnel destination	The NSAP address of the tunnel destination. The N-Selector part of the displayed NSAP address is set by the router and cannot be changed.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface. This counter is updated only when packets are process-switched, not when packets are fast-switched.
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. *** indicates that the elapsed time is too large to be displayed. 0:00:00 indicates that the counters were cleared more than 231 ms (and less than 232 ms) ago.
Queueing strategy	Type of queueing active on this interface.
Output queue, drops Input queue, drops	Number of packets in output and input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped because of a full queue.

Field	Description
Five minute input rate, Five minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes. The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of 4 time constants must pass before the average will be within 2 percent of the instantaneous rate of a uniform stream of traffic over that period.
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes in the error-free packets received by the system.
no buffer	Number of received packets discarded because there was no memory buffer available.
broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	This field does not apply to the CTunnel virtual interface.
giants	This field does not apply to the CTunnel virtual interface.
throttles	This field does not apply to the CTunnel virtual interface.
input errors	This field does not apply to the CTunnel virtual interface.
CRC	This field does not apply to the CTunnel virtual interface.
frame	This field does not apply to the CTunnel virtual interface.
overrun	This field does not apply to the CTunnel virtual interface.
ignored	This field does not apply to the CTunnel virtual interface.
abort	This field does not apply to the CTunnel virtual interface.
packets output	Total number of messages transmitted by the system.
bytes	Total number of bytes transmitted by the system.
underruns	This field does not apply to the CTunnel virtual interface.
output errors	This field does not apply to the CTunnel virtual interface.
collisions	This field does not apply to the CTunnel virtual interface.
interface resets	Number of times an interface has been reset. The interface may be reset manually by the administrator or automatically by the system when an internal error occurs.
output buffer failures	Number of buffer failures.
output buffers swapped out	Number of output buffer allocation failures.

Related Commands

Command	Description
show interfaces	Displays the statistical information specific to interfaces.

show interfaces debounce

To display the status and configuration for the debounce timer, use the **showinterfacesdebounce** command in user EXEC or privileged EXEC mode.

show interfaces [{*interface interface-number* | **null** *interface-number* | **vlan** *vlan-id*}] **debounce** [**module** *num*]

Syntax Description

interface	(Optional) Interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **port-channel**, **pos**, **atm**, and **ge-wan**.
interface-number	(Optional) Module and port number; see the "Usage Guidelines" section for valid values.
null *interface-number*	(Optional) Specifies the null interface; the valid value is **0**.
vlan *vlan-id*	(Optional) Specifies the VLAN; valid values are from 1 to 4094.
module *num*	(Optional) Limits the display to interfaces on the specified module.

Command Default

This command has no default settings.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **pos**, **atm**, and **ge-wan** keywords are supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

The debounce timer is not supported on the 10-Gigabit Ethernet module (WSX-6502-10GE).

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

The port-channel values are from 0 to 282; values from 257 to 282 are supported on the CSM and the FWSM only.

Examples

This example shows how to display the debounce configuration of an interface:

```
Router> show interfaces GigabitEthernet 1/1 debounce
Port   Debounce time   Value
```

```
Gi1/1   enable          100
Router>
```

Related Commands

Command	Description
link debounce	Enables the debounce timer on an interface.

show interfaces description

To display a description and a status of an interface, use the **showinterfacesdescription** command in user EXEC or privileged EXEC mode.

show interfaces [*interface*] **description**

Syntax Description

interface	(Optional) Interface type; for a list of valid values, see the "Usage Guidelines" section .

Command Default

This command has no default settings.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

When you enter the *interface* value, these formats can be used:

- *card-type slot* /*first-port* - *last-port*
- *card-type slot* /*first-port* - *last-port*

You can define a single port range per command entry. If you specify a range of ports, the range must consist of the same slot and port type. When you define a range, you must enter a space before and after the hyphen (-) as follows:

```
show interfaces gigabitethernet7/1 - 7 counters broadcast
```

Possible valid values for *card-type* are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **port-channel**, **pos**, **atm**, and **ge-wan**

The **pos**, **atm**, and **ge-wan** keywords are supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

The port-channel values are from 0 to 282; values from 257 to 282 are supported on the CSM and the FWSM only.

Examples

This example shows how to display the information for all interfaces:

```
Router> show interfaces description
 Interface Status         Protocol Description
 PO0/0     admin down     down     First POS interface
 PO0/1     admin down     down
 Gi1/0     up             up       GigE to server farm
Router>
```

Related Commands

Command	Description
description	Includes a specific description about the DSP interface.

show interfaces ethernet

To display information about an Ethernet interface on the router, use the **showinterfacesethernet** command in privileged EXEC mode.

Standard Syntax
show interfaces ethernet [*number*] [**accounting**]

Cisco 7200 and 7500 Series
show interfaces : ethernet accounting optionshow interfaces ethernet [*slot/port*] [**accounting**]

Cisco 7500 Series with Ports on VIPs
show interfaces ethernet [*slot/port-adapter/port*]

Catalyst 6500 Series Switches
show interfaces ethernet [**vlan** *vlan*]

Syntax Description

number	(Optional) Port number on the selected interface.
accounting	(Optional) Displays the number of packets of each protocol type that have been sent through the interface.
slot	(Optional) Slot number. Refer to the appropriate hardware manual for slot and port information.
/ *port*	(Optional) Port number. Refer to the appropriate hardware manual for slot and port information.
/ *port-adapter*	(Optional) Port adapter number. Refer to the appropriate hardware manual for information about port adapter compatibility.
vlan *vlan*	(Optional) Specifies a VLAN. Limits the display of switch port information to the specified VLAN. Range: 1 to 4094.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SXI	This command was changed to add the optional **vlan***vlan* keyword and argument.

Usage Guidelines

If you do not provide values for the *number*argument (or *slot*, *port*, and *port-adapter* arguments), the command displays statistics for all network interfaces. The optional keyword **accounting** displays the number of packets of each protocol type that have been sent through the interface.

Cisco IOS Release 12.2(33)SXI and later releases allow you to limit the display of switch port information to the specified VLAN.

Examples

The following is sample output from the **showinterfacesethernet**command for Ethernet interface 0:

```
Router# show interfaces ethernet 0
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 0060.3ef1.702b (bia 0060.3ef1.702b)
  Internet address is 172.21.102.33/24
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:20, output 00:00:06, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     115331 packets input, 27282407 bytes, 0 no buffer
     Received 93567 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     143782 packets output, 14482169 bytes, 0 underruns
     0 output errors, 1 collisions, 5 interface resets
     0 babbles, 0 late collision, 7 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

The table below describes significant fields shown in the display.

*Table 127: **show interfaces ethernet** Field Descriptions*

Field	Description
Ethernet ... is up ... is administratively down	Indicates whether the interface hardware is currently active and if it has been taken down by an administrator. “Disabled” indicates the router has received over 5000 errors in a keepalive interval, which is 10 seconds by default.
line protocol is {up | down | administratively down}	Indicates whether the software processes that handle the line protocol believe the interface is usable (that is, whether keepalives are successful) or if it has been taken down by an administrator.
Hardware	Hardware type (for example, MCI Ethernet, SCI, cBus Ethernet) and address.
Internet address	Internet address followed by subnet mask.
MTU	Maximum transmission unit of the interface.
BW	Bandwidth of the interface, in kilobits per second.
DLY	Delay of the interface, in microseconds.
rely	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.

Field	Description
load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method assigned to interface.
ARP type:	Type of Address Resolution Protocol assigned.
loopback	Indicates whether loopback is set or not.
keepalive	Indicates whether keepalives are set or not.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This counter is updated only when packets are process-switched, not when packets are fast-switched.
Last output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by an interface. This counter is updated only when packets are process-switched, not when packets are fast-switched.
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by the interface. Useful for knowing when a dead interface failed.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. *** indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 231 ms (and less than 232 ms) ago.
Output queue, input queue, drops	Number of packets in output and input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped because of a full queue.
5 minute input rate, 5 minute output rate	Average number of bits and packets transmitted per second in the last five minutes. If the interface is not in promiscuous mode, it senses network traffic it sends and receives (rather than all network traffic). The five-minute input and output rates should be used only as an approximation of traffic per second during a given five-minute period. These rates are exponentially weighted averages with a time constant of five minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.
packets input	Total number of error-free packets received by the system.

Field	Description
bytes input	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
no buffers	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernet networks and bursts of noise on serial lines are often responsible for no input buffer events.
Received ... broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium. For instance, any Ethernet packet that is less than 64 bytes is considered a runt.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium. For example, any Ethernet packet that is greater than 1518 bytes is considered a giant.
input error	Includes runts, giants, no buffer, CRC, frame, overrun, and ignored counts. Other input-related errors can also cause the input errors count to be increased, and some datagrams may have more than one error; therefore, this sum may not balance with the sum of enumerated input error counts.
CRC	Cyclic redundancy checksum generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a LAN, this is usually the result of collisions or a malfunctioning Ethernet device.
overrun	Number of times the receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be increased.
input packets with dribble condition detected	Dribble bit error indicates that a frame is slightly too long. This frame error counter is incremented just for informational purposes; the router accepts the frame.
packets output	Total number of messages transmitted by the system.
bytes	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the transmitter has been running faster than the router can handle. This may never be reported on some interfaces.

Field	Description
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors, as some datagrams may have more than one error, and others may have errors that do not fall into any of the specifically tabulated categories.
collisions	Number of messages transmitted because of an Ethernet collision. A packet that collides is counted only once in output packets.
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within several seconds. On a serial line, this can be caused by a malfunctioning modem that is not supplying the transmit clock signal, or by a cable problem. If the system notices that the carrier detect line of a serial interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an interface is looped back or shut down.
restarts	Number of times a Type 2 Ethernet controller was restarted because of errors.
babbles	The transmit jabber timer expired.
late collision	Number of late collisions. Late collision happens when a collision occurs after transmitting the preamble. The most common cause of late collisions is that your Ethernet cable segments are too long for the speed at which you are transmitting.
deferred	Deferred indicates that the chip had to defer while ready to transmit a frame because the carrier was asserted.
lost carrier	Number of times the carrier was lost during transmission.
no carrier	Number of times the carrier was not present during the transmission.
output buffer failures	Number of failed buffers and number of buffers swapped out.

Example on Cisco 7500 Series Routers

The following sample output illustrates the **showinterfacesethernet** command on a Cisco 7500 series router:

```
Router# show interfaces ethernet 4/2
Ethernet4/2 is up, line protocol is up
  Hardware is cxBus Ethernet, address is 0000.0c02.d0ce (bia 0000.0c02.d0ce)
  Internet address is 10.108.7.1, subnet mask is 255.255.255.0
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 4:00:00
  Last input 0:00:00, output 0:00:09, output hang never
  Last clearing of "show interface" counters 0:56:40
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  Five minute input rate 3000 bits/sec, 4 packets/sec
  Five minute output rate 0 bits/sec, 0 packets/sec
     4961 packets input, 715381 bytes, 0 no buffer
```

```
     Received 2014 broadcasts, 0 runts, 0 giants
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     567 packets output, 224914 bytes, 0 underruns
     0 output errors, 168 collisions, 0 interface resets, 0 restarts
     0 babbles, 2 late collision, 7 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Example with Accounting Option

The following is sample output from the **showinterfacesethernet** command with the **accounting** option on a Cisco 7500 series router:

```
Router# show interfaces ethernet 4/2 accounting
Ethernet4/2
       Protocol    Pkts In   Chars In   Pkts Out  Chars Out
             IP       7344    4787842       1803    1535774
      Appletalk      33345    4797459      12781    1089695
        DEC MOP          0          0        127       9779
            ARP          7        420         39       2340
```

The table below describes the fields shown in the display.

*Table 128: **show interfaces ethernet** Field Descriptions--Accounting*

Field	Description
Protocol	Protocol that is operating on the interface.
Pkts In	Number of packets received for that protocol.
Chars In	Number of characters received for that protocol.
Pkts Out	Number of packets transmitted for that protocol.
Chars Out	Number of characters transmitted for that protocol.

Catalyst 6500 Series Switches

The following is sample output from the **showinterfacesethernet**command for VLAN 2:

```
Router# show interfaces ethernet vlan 2
```

show interfaces fastethernet

To display information about the Fast Ethernet interfaces, use the **showinterfacesfastethernet** command in user EXEC or privileged EXEC mode.

Standard Syntax
show interfaces fastethernet [*number*]

Cisco 7200 and Cisco 7500 Series
show interfaces fastethernet [*slot*/*port*]

Cisco 7500 Series with a VIP
show interfaces fastethernet [*slot*/*port-adapter*/*port*]

Syntax Description

number	(Optional) Port, connector, or interface card number. On a Cisco 4700 series routers, specifies the network interface module (NIM) or NPM number. The numbers are assigned at the factory at the time of installation or when added to a system.
slot	(Optional) Slot number. Refer to the appropriate hardware manual for slot and port information.
port	(Optional) Port number. Refer to the appropriate hardware manual for slot and port information.
port-adapter	(Optional) Port adapter number. Refer to the appropriate hardware manual for information about port adapter compatibility.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **showinterfacesfastethernet** command on a Cisco 4700 series router:

```
Router# show interfaces fastethernet 0
Fast Ethernet0 is up, line protocol is up
  Hardware is DEC21140, address is 0000.0c0c.1111 (bia 0002.eaa3.5a60)
  Internet address is 10.0.0.1 255.0.0.0
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive not set, hdx, 100BaseTX
  ARP type: ARPA, ARP Timeout 4:00:00
  Last input never, output 0:00:16, output hang 0:28:01
  Last clearing of "show interface" counters 0:20:05
```

```
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants
     0 input errors, 0 CRC, 0 frame, 0 overrun, 1786161921 ignored, 0 abort
     0 watchdog, 0 multicast
     0 input packets with dribble condition detected
     67 packets output, 8151 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets, 0 restarts
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

The following is sample output from the **showinterfacesfastethernet** command on a Cisco AS5300 access server:

```
Router# show interfaces fastethernet 0
Fast Ethernet0 is up, line protocol is up
  Hardware is DEC21140AD, address is 00e0.1e3e.c179 (bia 00e0.1e3e.c179)
  Internet address is 10.17.30.4/16
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  Half-duplex, 10Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:03, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/120, 8 drops
  5 minute input rate 2000 bits/sec, 3 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     158773 packets input, 17362631 bytes, 4 no buffer
     Received 158781 broadcasts, 0 runts, 0 giants, 7 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast
     0 input packets with dribble condition detected
     6299 packets output, 622530 bytes, 0 underruns
     1 output errors, 0 collisions, 3 interface resets
     0 babbles, 0 late collision, 0 deferred
     1 lost carrier, 1 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

The following shows information specific to the first Fast Ethernet Interface Processor (FEIP) port in slot 0 on a Cisco 7500 series router:

```
Router# show interfaces fastethernet 0/1
Fast Ethernet0/1 is administratively down, line protocol is down
  Hardware is cxBus Fast Ethernet, address is 0000.0c35.dc16 (bia 0000.0c35.dc16)
  Internet address is 10.1.0.64 255.255.0.0
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive not set, half-duplex, RJ45 (or MII)
  ARP type: ARPA, ARP Timeout 4:00:00
  Last input never, output 2:03:52, output hang never
  Last clearing of "show interface" counters never
  Output queue 0/40, 0 drops; input queue 0/75, 1 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast
     0 input packets with dribble condition detected
     5 packets output, 805 bytes, 0 underruns
```

```
0 output errors, 0 collisions, 4 interface resets, 0 restarts
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
```

The table below describes the fields shown in these displays.

*Table 129: **show interfaces fastethernet** Field Descriptions*

Field	Description
Fast Ethernet0 is ... is up ...is administratively down	Indicates whether the interface hardware is currently active and if it has been taken down by an administrator.
line protocol is	Indicates whether the software processes that handle the line protocol consider the line usable or if it has been taken down by an administrator.
Hardware	Hardware type (for example, MCI Ethernet, SCI, cBus Ethernet) and address.
Internet address	Internet address followed by subnet mask.
MTU	Maximum transmission unit of the interface.
BW	Bandwidth of the interface, in kilobits per second.
DLY	Delay of the interface, in microseconds.
rely	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method assigned to interface.
ARP type	Type of Address Resolution Protocol assigned.
loopback	Indicates whether loopback is set or not.
keepalive	Indicates whether keepalives are set or not.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This counter is updated only when packets are process-switched, not when packets are fast-switched.
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by the interface. Useful for knowing when a dead interface failed. This counter is updated only when packets are process-switched, not when packets are fast-switched.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.

Field	Description
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. *** indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 231 ms (and less than 232 ms) ago.
Output queue, input queue, drops	Number of packets in output and input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped because of a full queue.
5 minute input rate, 5 minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic it sends and receives (rather than all network traffic). The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernets and bursts of noise on serial lines are often responsible for no input buffer events.
Received ... broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium. For instance, any Ethernet packet that is less than 64 bytes is considered a runt.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium. For example, any Ethernet packet that is greater than 1518 bytes is considered a giant.
input errors	Includes runts, giants, no buffer, CRC, frame, overrun, and ignored counts. Other input-related errors can also cause the input errors count to be increased, and some datagrams may have more than one error; therefore, this sum may not balance with the sum of enumerated input error counts.
CRC	Cyclic redundancy checksum generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data.

Field	Description
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a LAN, this is usually the result of collisions or a malfunctioning Ethernet device.
overrun	Number of times the receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be increased.
abort	Number of packets whose receipt was aborted.
watchdog	Number of times watchdog receive timer expired. It happens when receiving a packet with length greater than 2048.
multicast	Number of multicast packets received.
input packets with dribble condition detected	Dribble bit error indicates that a frame is slightly too long. This frame error counter is incremented just for informational purposes; the router accepts the frame.
packets output	Total number of messages transmitted by the system.
bytes	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the transmitter has been running faster than the router can handle. This may never be reported on some interfaces.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors, as some datagrams may have more than one error, and others may have errors that do not fall into any of the specifically tabulated categories.
collisions	Number of messages retransmitted because of an Ethernet collision. A packet that collides is counted only once in output packets.
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within several seconds. On a serial line, this can be caused by a malfunctioning modem that is not supplying the transmit clock signal, or by a cable problem. If the system notices that the carrier detect line of a serial interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an interface is looped back or shut down.
restarts	Number of times a Type 2 Ethernet controller was restarted because of errors.
babbles	The transmit jabber timer expired.

Field	Description
late collision	Number of late collisions. Late collision happens when a collision occurs after transmitting the preamble. The most common cause of late collisions is that your Ethernet cable segments are too long for the speed at which you are transmitting.
deferred	Deferred indicates that the chip had to defer while ready to transmit a frame because the carrier was asserted.
lost carrier	Number of times the carrier was lost during transmission.
no carrier	Number of times the carrier was not present during the transmission.
output buffer failures	Number of failed buffers and number of buffers swapped out.

The following example of the **showinterfacesfastethernet**command shows all the information specific to the first PA-12E/2FE interface port (interface port 0) in port adapter slot 3:

```
Router# show interfaces fastethernet 3/0
Fast Ethernet3/0 is up, line protocol is up
  Hardware is TSWITCH, address is 00e0.f7a4.5130 (bia 00e0.f7a4.5130)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  Half-duplex, 100BaseTX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:05:30, output 00:00:00, output hang never
  Last clearing of “show interface” counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     312 packets input, 18370 bytes, 0 no buffer
     Received 216 broadcasts, 0 runts, 0 giants, 0 throttles
     3 input errors, 0 CRC, 0 frame, 0 overrun, 3 ignored, 0 abort
     0 input packets with dribble condition detected
     15490 packets output, 1555780 bytes, 0 underruns
     2 output errors, 0 collisions, 2 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     2 output buffer failures, 0 output buffers swapped out
```

The table below describes the fields shown in this display.

Table 130: show interfaces fastethernet Field Descriptions--PA-12E/2FE

Field	Description
Fast Ethernet... is up ...is administratively down	Indicates whether the interface hardware is currently active and if it has been taken down by an administrator.
line protocol is	Indicates whether the software processes that handle the line protocol consider the line usable or if it has been taken down by an administrator.
Hardware	Hardware type (for example, MCI Ethernet, SCI, cBus Ethernet) and address.
Internet address	Internet address followed by subnet mask.
MTU	Maximum transmission unit of the interface.

Field	Description
BW	Bandwidth of the interface, in kilobits per second.
DLY	Delay of the interface, in microseconds.
rely	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method assigned to interface.
ARP type	Type of Address Resolution Protocol assigned.
loopback	Indicates whether loopback is set or not.
keepalive	Indicates whether keepalives are set or not.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This counter is updated only when packets are process-switched, not when packets are fast-switched.
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by the interface. Useful for knowing when a dead interface failed.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the “last” fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. *** indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 231 ms (and less than 232 ms) ago.
Output queue, input queue, drops	Number of packets in output and input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped because of a full queue.

Field	Description
5 minute input rate, 5 minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic it sends and receives (rather than all network traffic). The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernets and bursts of noise on serial lines are often responsible for no input buffer events.
Received ... broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium. For instance, any Ethernet packet that is less than 64 bytes is considered a runt.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium. For example, any Ethernet packet that is greater than 1518 bytes is considered a giant.
throttles	Number of times the receiver on the port was disabled, possibly because of buffer or processor overload.
input errors	Includes runts, giants, no buffer, CRC, frame, overrun, and ignored counts. Other input-related errors can also cause the input errors count to be increased, and some datagrams may have more than one error; therefore, this sum may not balance with the sum of enumerated input error counts.
CRC	Cyclic redundancy checksum generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a LAN, this is usually the result of collisions or a malfunctioning Ethernet device.
overrun	Number of times the receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.

Field	Description
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be increased.
abort	Number of packets whose receipt was aborted.
input packets with dribble condition detected	Dribble bit error indicates that a frame is slightly too long. This frame error counter is incremented for informational purposes; the router accepts the frame.
packets output	Total number of messages transmitted by the system.
bytes	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the transmitter has been running faster than the router can handle. This may never be reported on some interfaces.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors, as some datagrams may have more than one error, and others may have errors that do not fall into any of the specifically tabulated categories.
collisions	Number of messages retransmitted because of an Ethernet collision. A packet that collides is counted only once in output packets.
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within several seconds. On a serial line, this can be caused by a malfunctioning modem that is not supplying the transmit clock signal, or by a cable problem. If the system notices that the carrier detect line of a serial interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an interface is looped back or shut down.
babbles	Transmit jabber timer expired.
late collision	Number of late collisions. Late collision happens when a collision occurs after transmitting the preamble. The most common cause of late collisions is that your Ethernet cable segments are too long for the speed at which you are transmitting.
deferred	Deferred indicates that the chip had to defer while ready to transmit a frame because the carrier was asserted.
lost carrier	Number of times the carrier was lost during transmission.
no carrier	Number of times the carrier was not present during the transmission.

show interfaces fddi

To display information about the FDDI interface, use the **showinterfacesfddi**command in user EXEC or privileged EXEC mode.

Standard Syntax
show interfaces fddi *number* [**accounting**]

Cisco 7000 and Cisco 7200 Series
show interfaces : fddi accounting optionshow interfaces fddi [*slot*/*port*] [**accounting**]

Cisco 7500 Series
show interfaces fddi [*slot*/*port-adapter*/*port*] [**accounting**]

Syntax Description

number	Port number on the selected interface.
accounting	(Optional) Displays the number of packets of each protocol type that have been sent through the interface.
slot	(Optional) Slot number. Refer to the appropriate hardware manual for slot and port information.
port	(Optional) Port number. Refer to the appropriate hardware manual for slot and port information.
port-adapter	(Optional) Port adapter number. Refer to the appropriate hardware manual for information about port adapter compatibility.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
11.3	This command was modified to include support for FDDI full-duplex, single- and multimode port adapters (PA-F/FD-SM and PA-F/FD-MM).
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is a sample partial display of FDDI-specific data from the **showinterfacesfddi** command on a Cisco 7500 series router:

```
Router# show interfaces fddi 3/0/0

Fddi3/0/0 is up, line protocol is up
  Hardware is cxBus Fddi, address is 0000.0c02.adf1 (bia 0000.0c02.adf1)
  Internet address is 10.108.33.14, subnet mask is 255.255.255.0
```

```
  MTU 4470 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation SNAP, loopback not set, keepalive not set
  ARP type: SNAP, ARP Timeout 4:00:00
  Phy-A state is active, neighbor is   B, cmt signal bits 008/20C, status ILS
  Phy-B state is active, neighbor is   A, cmt signal bits 20C/008, status ILS
  ECM is in, CFM is thru, RMT is ring_op
  Token rotation 5000 usec, ring operational 21:32:34
  Upstream neighbor 0000.0c02.ba83, downstream neighbor 0000.0c02.ba83
  Last input 0:00:05, output 0:00:00, output hang never
  Last clearing of "show interface" counters 0:59:10
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  Five minute input rate 69000 bits/sec, 44 packets/sec
  Five minute output rate 0 bits/sec, 1 packets/sec
     113157 packets input, 21622582 bytes, 0 no buffer
     Received 276 broadcasts, 0 runts, 0 giants
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     4740 packets output, 487346 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets, 0 restarts
     0 transitions, 2 traces, 3 claims, 2 beacons
```

The following is sample output from the **showinterfacesfddi**command for the full-duplex FDDI port adapter on a Cisco 7500 series router:

```
Router# show interfaces fddi 0/1/0
Fddi0/1/0 is up, line protocol is up
  Hardware is cxBus FDDI, address is 0060.3e33.3608 (bia 0060.3e33.3608)
  Internet address is 10.1.1.1/24
  MTU 4470 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation SNAP, loopback not set, keepalive not set
  ARP type: SNAP, ARP Timeout 04:00:00
  FDX supported, FDX enabled, FDX state is operation
  Phy-A state is maintenance, neighbor is Unknown, status HLS
  Phy-B state is active, neighbor is A, status SILS
  ECM is in, CFM is c_wrap_b, RMT is ring_op,
  Requested token rotation 5000 usec, negotiated 4997 usec
  Configured tvx is 2500 usec
  LER for PortA = 0A, LER for PortB = 0A ring operational 00:02:45
  Upstream neighbor 0060.3e73.4600, downstream neighbor 0060.3e73.4600
  Last input 00:00:12, output 00:00:13, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     62 packets input, 6024 bytes, 0 no buffer
     Received 18 broadcasts, 0 runts, 0 giants
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     71 packets output, 4961 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     3 transitions, 0 traces, 100 claims, 0 beacon
```

The table below describes thefields shown in the display.

Table 131: show interfaces fddi Field Descriptions

Field	Description
Fddi is {up | down | administratively down	Gives the interface processor unit number and tells whether the interface hardware is currently active and can transmit and receive or if it has been taken down by an administrator.

Field	Description
line protocol is {up | down}	Indicates whether the software processes that handle the line protocol consider the interface usable.
Hardware	Provides the hardware type, followed by the hardware address.
Internet address	IP address, followed by subnet mask.
MTU	Maximum transmission unit of the interface.
BW	Bandwidth of the interface, in kilobits per second.
DLY	Delay of the interface, in microseconds.
rely	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method assigned to interface.
loopback	Indicates whether or not loopback is set.
keepalive	Indicates whether or not keepalives are set.
ARP type	Type of Address Resolution Protocol assigned.
FDX	Displays full-duplex information. Values are: not supported or supported. When the value is supported, the display indicates whether full-duplex is enabled or disabled. When enabled, the state of the FDX negotiation process is displayed. The negotiation states only relate to the full-duplex negotiation process. You must also ensure that the interface is up and working by looking at other fields in the **showinterfacesfddi** command such as line protocol and RMT. Negotiation states are: • idle--Interface is working but not in full-duplex mode yet. If persistent, it could mean that the interface did not meet all negotiation conditions (for example, there are more than two stations in the ring). • request--Interface is working but not in full-duplex mode yet. If persistent, it could mean that the remote interface does not support full-duplex or full-duplex is not enabled on the interface. • confirm--Transient state. • operation--Negotiations completed successfully, and both stations are operating in full-duplex mode.
Phy-{A | B}	Lists the state the Physical A or Physical B connection is in; one of the following: off, active, trace, connect, next, signal, join, verify, or break.

Field	Description
neighbor	State of the neighbor: • A--Indicates that the connection management (CMT) process has established a connection with its neighbor. The bits received during the CMT signaling process indicate that the neighbor is a Physical A type dual attachment station (DAS) or concentrator that attaches to the primary ring IN and the secondary ring OUT when attaching to the dual ring. • S--Indicates that the CMT process has established a connection with its neighbor and that the bits received during the CMT signaling process indicate that the neighbor is one Physical type in a single attachment station (SAS). • B--Indicates that the CMT process has established a connection with its neighbor and that the bits received during the CMT signaling process indicate that the neighbor is a Physical B dual attachment station or concentrator that attaches to the secondary ring IN and the primary ring OUT when attaching to the dual ring. • M--Indicates that the CMT process has established a connection with its neighbor and that the bits received during the CMT signaling process indicate that the router's neighbor is a Physical M-type concentrator serving as a Master to a connected station or concentrator. • unk--Indicates that the network server has not completed the CMT process and, as a result, does not know about its neighbor. See the section "Setting Bit Control" for an explanation of the bit patterns.
cmt signal bits	Shows the transmitted/received CMT bits. The transmitted bits are 0x008 for a Physical A type and 0x20C for Physical B type. The number after the slash (/) is the received signal bits. If the connection is not active, the received bits are zero (0); see the line beginning Phy-B in the display. This applies to FIP interfaces only.

Field	Description
status	Status value displayed is the actual status on the fiber. The FDDI standard defines the following values: • LSU--Line State Unknown, the criteria for entering or remaining in any other line state have not been met. • NLS--Noise Line State is entered upon the occurrence of 16 potential noise events without satisfying the criteria for entry into another line state. • MLS--Master Line State is entered upon the receipt of eight or nine consecutive HQ or QH symbol pairs. • ILS--Idle Line State is entered upon receipt of four or five idle symbols. • HLS--Halt Line State is entered upon the receipt of 16 or 17 consecutive H symbols. • QLS--Quiet Line State is entered upon the receipt of 16 or 17 consecutive Q symbols or when carrier detect goes low. • ALS--Active Line State is entered upon receipt of a JK symbol pair when carrier detect is high. • OVUF--Elasticity buffer Overflow/Underflow. The normal states for a connected Physical type are ILS or ALS. If the report displays the QLS status, this indicates that the fiber is disconnected from Physical B, or that it is not connected to another Physical type, or that the other station is not running.
ECM is...	ECM is the SMT entity coordination management, which overlooks the operation of CFM and PCM. The ECM state can be one of the following: • out--Router is isolated from the network. • in--Router is actively connected to the network. This is the normal state for a connected router. • trace--Router is trying to localize a stuck beacon condition. • leave--Router is allowing time for all the connections to break before leaving the network. • path_test--Router is testing its internal paths. • insert--Router is allowing time for the optical bypass to insert. • check--Router is making sure optical bypasses switched correctly. • deinsert--Router is allowing time for the optical bypass to deinsert.

Field	Description
CFM is...	Contains information about the current state of the MAC connection. The Configuration Management state can be one of the following: • isolated--MAC is not attached to any Physical type. • wrap_a--MAC is attached to Physical A. Data is received on Physical A and transmitted on Physical A. • wrap_b--MAC is attached to Physical B. Data is received on Physical B and transmitted on Physical B. • wrap_s--MAC is attached to Physical S. Data is received on Physical S and transmitted on Physical S. This is the normal mode for a single attachment station (SAS). • thru--MAC is attached to Physical A and B. Data is received on Physical A and transmitted on Physical B. This is the normal mode for a dual attachment station (DAS) with one MAC. The ring has been operational for 1 minute and 42 seconds.
RMT is...	RMT (Ring Management) is the SMT MAC-related state machine. The RMT state can be one of the following: • isolated--MAC is not trying to participate in the ring. This is the initial state. • non_op--MAC is participating in ring recovery, and ring is not operational. • ring_op--MAC is participating in an operational ring. This is the normal state while the MAC is connected to the ring. • detect--Ring has been nonoperational for longer than normal. Duplicate address conditions are being checked. • non_op_dup--Indications have been received that the address of the MAC is a duplicate of another MAC on the ring. Ring is not operational. • ring_op_dup--Indications have been received that the address of the MAC is a duplicate of another MAC on the ring. Ring is operational in this state. • directed--MAC is sending beacon frames notifying the ring of the stuck condition. • trace--Trace has been initiated by this MAC, and the RMT state machine is waiting for its completion before starting an internal path test.
token rotation	Token rotation value is the default or configured rotation value as determined by the **fdditoken-rotation-time** command. This value is used by all stations on the ring. The default is 5000 microseconds. For FDDI full-duplex, this indicates the value in use prior to entering full-duplex operation.
negotiated	Actual (negotiated) target token rotation time.
ring operational	When the ring is operational, the displayed value will be the negotiated token rotation time of all stations on the ring. Operational times are displayed by the number of hours:minutes:seconds the ring has been up. If the ring is not operational, the message “ring not operational” is displayed.

Field	Description
Configured tvx	Transmission timer.
LER	Link error rate.
Upstream | downstream neighbor	Displays the canonical MAC address of outgoing upstream and downstream neighbors. If the address is unknown, the value will be the FDDI unknown address (0x00 00 f8 00 00 00).
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This counter is updated only when packets are process-switched, not when packets are fast-switched.
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by an interface. This counter is updated only when packets are process-switched, not when packets are fast-switched.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. *** indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 231 ms (and less than 232 ms) ago.
Queueing strategy	First-in, first-out queueing strategy (other queueing strategies you might see are priority-list, custom-list, and weighted fair).
Output queue, input queue, drops	Number of packets in output and input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped because of a full queue.
5 minute input rate 5 minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes. The five-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.

Field	Description
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernet networks and bursts of noise on serial lines are often responsible for no input buffer events.
broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the media.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium.
CRC	Cyclic redundancy checksum generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data.
frame	Number of packets received incorrectly that have a CRC error and a noninteger number of octets. On a LAN, this is usually the result of collisions or a malfunctioning Ethernet device. On an FDDI LAN, this also can be the result of a failing fiber (cracks) or a hardware malfunction.
overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different from the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be increased.
packets output	Total number of messages transmitted by the system.
bytes	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of transmit aborts (when the router cannot feed the transmitter fast enough).
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this might not balance with the sum of the enumerated output errors, because some datagrams can have more than one error, and others can have errors that do not fall into any of the specifically tabulated categories.
collisions	Because an FDDI ring cannot have collisions, this statistic is always zero.
interface resets	Number of times an interface has been reset. The interface may be reset by the administrator or automatically when an internal error occurs.
restarts	Should always be zero for FDDI interfaces.

Field	Description
output buffer failures	Number of no resource errors received on the output.
output buffers swapped out	Number of packets swapped to DRAM.
transitions	The number of times the ring made a transition from ring operational to ring nonoperational, or vice versa. A large number of transitions indicates a problem with the ring or the interface.
traces	Trace count applies to both the FCI, FCIT, and FIP. Indicates the number of times this interface started a trace.
claims	Pertains to FCIT and FIP only. Indicates the number of times this interface has been in claim state.
beacons	Pertains to FCIT and FIP only. Indicates the number of times the interface has been in beacon state.

The following is sample output that includes the **accounting** option. When you use the **accounting** option, only the accounting statistics are displayed.

```
Router# show interfaces fddi 3/0 accounting
Fddi3/0
       Protocol    Pkts In   Chars In   Pkts Out  Chars Out
             IP       7344    4787842       1803    1535774
     Appletalk       33345    4797459      12781    1089695
        DEC MOP          0          0        127       9779
            ARP          7        420         39       2340
```

The table below describes thefields shown in the display.

*Table 132: **show interfaces fddi** Field Descriptions--Accounting*

Field	Description
Protocol	Protocol that is operating on the interface.
Pkts In	Number of packets received for that protocol.
Chars In	Number of characters received for that protocol.
Pkts Out	Number of packets transmitted for that protocol.
Chars Out	Number of characters transmitted for that protocol.

show interfaces flowcontrol

To display flow-control information, use the **showinterfacesflowcontrol** command in user EXEC or privileged EXEC mode.

show interfaces [*interface* [*mod*]] **flowcontrol** [{**module** *number* | **vlan** *vlan*}]

Syntax Description

interface	(Optional) Interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **port-channel**, **vlan** , **pos**, **atm**, and **ge-wan** **Note** The show interfaces vlan vlan flowcontrol command displays the interface VLAN information.
mod	(Optional) Module and port number.
module *number*	(Optional) Specifies the module number; see the "Usage Guidelines" section for valid values.
vlan **Note** The show interfaces flowcontrol vlan vlan command limits the display to interfaces on the specified VLAN.	(Optional) Limits the display of switch port information to the specified VLAN. Range: 1 to 4094

Command Default

This command has no default settings.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXI	This command was changed to add the optional **vlan***vlan* keyword and argument.

Usage Guidelines

The **pos**, **atm**, and **ge-wan** keywords are supported on systems that are configured with a Supervisor Engine 2

The *mod*argument designates the module and port number. Valid values for *mod* depend on the chassis and module that are used. For example, if you have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the slot number are from 1 to 13 and valid values for the port number are from 1 to 48.

The **module***number* keyword and argument designate the module number and limit the display to interfaces on the module. Valid values depend on the chassis that is used. For example, if you have a 13-slot chassis, valid values for the module number are from 1 to 13.

The port-channel values are from 0 to 282; values from 257 to 282 are supported on the CSM and the FWSM only.

Cisco IOS Release 12.2(33)SXI and later releases allow you to limit the display of switch port information to the specified VLAN.

Examples

This example shows how to display flow-control information for all interfaces:

```
Router> show interfaces flowcontrol
Port  Send    FlowControl Receive FlowControl RxPause TxPause
      admin     oper      admin     oper
----- --------  --------  --------  --------  -------  -------
Gi1/1 desired   off       off       off       0        0
Gi1/2 desired   off       off       off       0        0
Gi3/1 on        on        on        on        0        0
.
.
.
Gi8/2 desired   off       off       off       0        0
Gi8/3 desired   off       off       off       0        0
Gi8/4 desired   off       off       off       0        0
Router>
```

This example shows how to display flow-control information for a specific interface:

```
Router> show interfaces gigabitethernet 8/2 flowcontrol
Port  Send    FlowControl Receive FlowControl RxPause TxPause
      admin     oper      admin     oper
----- --------  --------  --------  --------  -------  -------
Gi8/2 desired   off       off       off       0        0
Router>
```

This example shows how to limit the display flow-control information for interfaces on a specific VLAN:

```
Router> show interfaces flowcontrol vlan 22
Router>
```

The table below describes the fields that are shown in the example.

Table 133: show port flowcontrol Command Output Fields

Field	Description
Port	Interface type and module and port number.
Send admin	Flow-control operation for admin state. Possible settings: on indicates that the local port is allowed to send pause frames to remote ports; off indicates that the local port is prevented from sending pause frames to remote ports; desired indicates predictable results whether a remote port is set to **receiveon**, **receiveoff**, or **receivedesired**.

Field	Description
Send oper	Current flow-control operation. Possible settings: on indicates that the local port is allowed to send pause frames to remote ports; off indicates that the local port is prevented from sending pause frames to remote ports; desired indicates predictable results whether a remote port is set to **receiveon**, **receiveoff**, or **receivedesired**.
Receive admin	Flow-control operation for admin state. Possible settings: on indicates that the local port is allowed to process pause frames that a remote port sends; off indicates that the local port is prevented from sending pause frames to remote ports; desired indicates predictable results whether a remote port is set to **sendon**, **sendoff**, or **senddesired**.
Receive oper	Current flow-control operation. Possible settings: on indicates that the local port is allowed to process pause frames that a remote port sends; off indicates that the local port is prevented from sending pause frames to remote ports; desired indicates predictable results whether a remote port is set to **sendon**, **sendoff**, or **senddesired**.
RxPause	Number of pause frames that are received.
TxPause	Number of pause frames that are transmitted.

Related Commands

Command	Description
flowcontrol	Configures a port to send or receive pause frames.

show interfaces gigabitethernet

To check the status of and configuration settings on a router that supports Gigabit Ethernet Shared Port Adapters (SPA), use the **show interfaces gigabitethernet** command in the privileged EXEC mode.

Cisco 7200 Series Router
show interfaces gigabitethernet *slot/port*

Cisco ASR 1000 Series Aggregation Services Router
show interfaces gigabitethernet *slot/subslot/port*

Syntax Description

slot	Chassis slot number. (Refer to the appropriate hardware manual for slot information. For SPA Interface Processors (SIPs), refer to the platform-specific SPA hardware installation guide or the platform-specific SPA software configuration guide.)
subslot	Secondary slot number on a SIP in which a SPA is installed. (Refer to the platform-specific SPA hardware installation guide or the platform-specific SPA software configuration guide for subslot information.)
port	Port number or interface number. (Refer to the appropriate hardware manual for port information. For SPAs, refer to the platform-specific SPA software configuration guide.)

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.1CC	This command was introduced.
12.1(3A)E	The command was modified to support Cisco 7200-I/O-GE+E Controller.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(20)S2	This command was integrated into Cisco IOS Release 12.2(20)S2. It was modified to include a new address format and output for the interfaces on the 2-port 10/100/1000 Gigabit Ethernet SPA on the Cisco 7304 Routers. The *subslot* argument was also added.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S to support the Gigabit Ethernet SPAs on the Cisco 12000 Series Routers.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF to support the Gigabit Ethernet SPAs on the Cisco 7600 Series Routers and the Cisco Catalyst 6500 Series Switches.
Cisco IOS XE Release 2.1	This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

This command is used in Cisco 7200-I/O-GE+E Controller and the Cisco ASR 1000 Series Aggregation Services Routers to display the configuration status of a Gigabit Ethernet interface.

> **Note:** On Cisco 7200-I/O-GE+E Controller, *slot 0* is always reserved for the Gigabit Ethernet port on the I/O controller.

Cisco 7200-I/O-GE+E Controller Example

The following is sample output from the **show interfaces gigabitethernet** command:

```
Router# show interfaces gigabitethernet 5/1

GigabitEthernet5/1 is up, line protocol is up
Hardware is C6k 1000Mb 802.3, address is 0015.c620.b580 (bia 0015.c620.b580)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s
  input flow-control is off, output flow-control is off
  Clock mode is auto
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

Cisco ASR 1000 Series Aggregation Services Router Example

The following is sample output from the **show interfaces gigabitethernet** command:

```
Router# show interface gigabitethernet 0/0/0

GigabitEthernet0/0/0 is up, line protocol is up
  Hardware is SPA-2X1GE-V2, address is 001f.6c25.c400 (bia 001f.6c25.c400)
  Description: Connected to CE28_C2811 GE 0/0/0
  Internet address is 192.168.128.43/24
  MTU 2000 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full Duplex, 1000Mbps, link type is auto, media type is SX
  output flow-control is on, input flow-control is on
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:46, output 00:09:07, output hang never
```

```
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     673295 packets input, 70811204 bytes, 0 no buffer
     Received 1 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 104296 multicast, 0 pause input
     1310016 packets output, 99574303 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

Gigabit Ethernet SPA Example

The following is sample output from the **show interfaces gigabitethernet** command for the first interface *port 0* in a 2-port 10/100/1000 Gigabit Ethernet SPA located in the top *subslot 0* of the MSC that is installed in *slot 4* on a Cisco 7304 Router:

```
Router# show interfaces gigabitethernet 4/0/0

GigabitEthernet4/0/0 is up, line protocol is down
  Hardware is SPA-2GE-7304, address is 00b0.64ff.5a80 (bia 00b0.64ff.5a80)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 1000Mb/s, link type is auto, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:09, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     109 packets output, 6540 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 babbles, 0 late collision, 0 deferred
     1 lost carrier, 0 no carrier, 0 PAUSE output
     0 output buffer failures, 0 output buffers swapped out
```

Note There will be variations in the output of the **show interfaces** command, depending on the platform, type of interface, and other features that you might have configured, such as Quality of Service (QoS). Therefore, some additional output fields might appear in your **show interfaces** command output. For more information about these fields, see the **show interfaces** command description in the *Cisco IOS Interface and Hardware Component Command Reference* document at: http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-s4.html#wp2987586133

The following table describes the significant fields shown in the displays:

Table 134: show interfaces gigabitethernet Field Descriptions

Field	Description
GigabitEthernet...is up ...is administratively down	Indicates whether the interface hardware is currently active or if it has been taken down by an administrator.
line protocol is	Indicates whether the software processes that handle the line protocol consider the line usable, or if it has been taken down by an administrator.
Hardware	Hardware type, for example, SPA-2GE-7304, and MAC address.
Description	Alphanumeric string identifying the interface. It is displayed only if the **description** interface configuration command has been configured on the interface.
Internet address	Internet address followed by the subnet mask.
MTU	Maximum transmission unit of the interface. The default is 1500 bytes for the 2-port 10/100/1000 Gigabit Ethernet SPA.
BW	Bandwidth of the interface, in kilobits, per second.
DLY	Delay in the interface, in microseconds.
reliability	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
txload, rxload	Load on the interface (in the transmit "tx" and receive "rx" directions) as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method assigned to the interface.
loopback	Indicates whether or not loopback is set.
Keepalive	Indicates whether or not keepalives are set, and the time interval.
Half-duplex, Full-duplex	Indicates the duplex mode of the interface.
1000Mb/s, 100Mb/s, 10Mb/s	Speed of the interface, in megabits, per second.
link type	Specifies whether or not auto negotiation is being used on the link.
media type	Interface port media type: RJ45, SX, LX, or ZX.
ARP type	Type of Address Resolution Protocol (ARP) assigned, and the timeout period.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by the interface and processed locally on a router. Useful for knowing when a dead interface failed. This field is not updated by fast-switched traffic.

Field	Description
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by the interface. Useful for knowing when a dead interface failed.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is displayed. If that field overflows, asterisks are displayed. **Note** This field does not apply to the SPA interfaces.
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in the report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. A series of asterisks (***) indicates that the elapsed time is too large to be displayed. 0:00:00 indicates that the counters were cleared more than 231 ms (and less than 232 ms) ago.
Input queue (size/max/drops/flushes)	Packet statistics on the input queue are reported as: • Size—Number of packets in the input queue. • Max—Maximum size of the queue. • Drops—Number of packets dropped because of a full input queue. • Flushes—Number of packets dropped as part of selective packet discard (SPD). SPD implements a selective packet drop policy on a router's IP process queue. Therefore, it only applies to process-switched traffic.
Total output drops	Total number of packets dropped because of a full output queue.
Queueing strategy	Type of Layer 3 queueing active on this interface. The default is first-in, first-out (FIFO).
Output queue (size/max)	Number of packets in the output queue (size), and the maximum size of the queue (max).
5 minute input rate, 5 minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes. If the interface is not in the promiscuous mode, it senses the network traffic it sends and receives (rather than all the network traffic). The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average can be within two percent of the instantaneous rate of a uniform stream of traffic over that period.
packets input	Total number of error-free packets received by the system.

Field	Description
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
Received...broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium. For instance, any Ethernet packet that is smaller than 64 bytes is considered a runt.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium. For example, any Ethernet packet that is larger than 1536 bytes is considered a giant. **Note** In the 2-port 10/100/1000 Gigabit Ethernet SPA, the default is that a giant is any packet greater than 1536 bytes. However, if you modify the maximum transmission unit (MTU) for the interface, this counter increments when you exceed the specified MTU for the interface.
throttles	Number of times the receiver on the port was disabled, possibly because of buffer or processor overload.
input errors	Includes runts, giants, no buffer, cyclic redundancy check (CRC), frame, overrun, oversubscription counters, and ignored counts. Other input-related errors can also cause the input errors count to be increased, and some datagrams may have more than one error. Therefore, this sum may not balance with the sum of enumerated input error counts. **Note** The oversubscription counters are included only on the Cisco ASR 1000 Series Aggregation Services Routers.
CRC	Cyclic redundancy check generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a LAN, this is usually the result of collisions or a malfunctioning Ethernet device.
overrun	Number of times the receiver hardware was unable to hand the received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data. The overrun also includes the interface oversubscription counters. **Note** The interface oversubscription counters are included only on the Cisco ASR 1000 Series Aggregation Services Routers.
ignored	Number of received packets ignored by the interface because the interface hardware is running low on internal buffers. These buffers are different from the system buffers. Broadcast storms and bursts of noise may cause the ignored count to be increased.

Field	Description
watchdog	Number of times the watchdog receive timer expires. Expiration occurs when receiving a packet with a length that is greater than 2048 bytes.
input packets with dribble condition detected	Dribble bit error indicates that a frame is slightly longer than usual. This frame error counter is incremented for informational purposes only; the router accepts the frame.
packets output	Total number of messages transmitted by the system.
bytes	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times the transmitter has been running faster than the speed a router can handle.
output errors	Sum of all the errors that prevented the final transmission of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors because some datagrams may have more than one error and others may have errors that do not fall into any of the specifically tabulated categories.
collisions	Number of messages retransmitted because of an Ethernet collision. This is usually the result of an overextended LAN, for example, an Ethernet or transceiver cable that is too long, more than two repeaters between stations, or too many cascaded multiport transceivers. A packet that collides is counted only once in output packets.
interface resets	Number of times an interface is completely reset. This may occur if packets that are queued for transmission were not sent within several seconds. Interface resets may occur when an interface is looped back or shut down.
babbles	Transmit jabber timer expired.
late collision	Number of late collisions. Late collision occurs when a collision takes place after the preamble is transmitted.
deferred	Number of times the interface had to defer while ready to transmit a frame because the carrier was asserted.
lost carrier	Number of times the carrier was lost during transmission.
no carrier	Number of times the carrier was not present during the transmission. **Note** This field does not apply to SPA interfaces.
output buffer failures, output buffers swapped out	These counters are not used by the 2-port 10/100/1000 Gigabit Ethernet SPA on the Cisco 7304 Routers.

Related Commands

Command	Description
show controllers gigabitethernet	Displays Gigabit Ethernet interface information, transmission statistics and errors, and applicable MAC destination address and VLAN filtering tables.
show interfaces	Displays the statistics for the interfaces configured on a router, switch, or access server.

show interfaces hssi

To display information about the high-speed serial interface (HSSI), use the **showinterfaceshssi**command in privileged EXEC mode.

Standard Syntax
show interfaces hssi *number* [**accounting**]

Cisco 7500 Series
show interfaces hssi [*slot*/*port*] [**accounting**]

Syntax Description

number	Port number on the selected interface.
accounting	(Optional) Displays the number of packets of each protocol type that have been sent through the interface.
slot	(Optional) Slot number. Refer to the appropriate hardware manual for slot and port information.
port	(Optional) Port number. Refer to the appropriate hardware manual for slot and port information.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **showinterfaceshssi** command when HSSI is enabled:

```
Router# show interfaces hssi 0
HSSI 0 is up, line protocol is up
 Hardware is cBus HSSI
 Internet address is 10.136.67.190, subnet mask is 255.255.255.0
 MTU 4470 bytes, BW 45045 Kbit, DLY 20000 usec, rely 255/255, load 1/255
 Encapsulation HDLC, loopback not set, keepalive set (10 sec)
 Last input 0:00:03, output 0:00:00, output hang never
 Output queue 0/40, 0 drops; input queue 0/75, 0 drops
 Five minute input rate 0 bits/sec, 0 packets/sec
 Five minute output rate 0 bits/sec, 0 packets/sec
      0 packets input, 0 bytes, 0 no buffer
      Received 0 broadcasts, 0 runts, 0 giants
              0 parity, 0 rx disabled
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 17 packets output, 994 bytes, 0 underruns
 0 output errors, 0 applique, 4 interface resets, 0 restarts
 2 carrier transitions
```

The table below describes significant fields shown in the display.

*Table 135: **show interfaces hssi** Field Descriptions*

Field	Description
HSSI is {up | down | administratively down}	Indicates whether the interface hardware is currently active (whether carrier detect is present) and whether it has been taken down by an administrator. "Disabled" indicate that the router has received over 5000 errors in a keepalive interval, which is 10 seconds by default.
line protocol is {up | down | administratively down}	Indicates whether the software processes that handle the line protocol consider the line usable (that is, whether keepalives are successful).
Hardware	Specifies the hardware type.
Internet address	Lists the Internet address followed by subnet mask.
MTU	Maximum transmission unit of the interface.
BW	Bandwidth of the interface, in kilobits per second.
DLY	Delay of the interface, in microseconds.
rely	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method assigned to interface.
loopback	Indicates whether loopback is set and type of loopback test.
keepalive	Indicates whether keepalives are set or not.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This counter is updated only when packets are process-switched, not when packets are fast-switched.
Last output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by an interface. This counter is updated only when packets are process-switched, not when packets are fast-switched.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.

Field	Description
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. *** indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 231 ms (and less than 232 ms) ago.
Output queue, drops Input queue, drops	Number of packets in output and input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped because of a full queue.
Five minute input rate, Five minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes.
packets input	Total number of error-free packets received by the system.
bytes input	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernet networks and bursts of noise on serial lines are often responsible for no input buffer events.
broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium.
parity	Report of the parity errors on the HSSI.
rx disabled	Indicates that the HSSI could not find a free buffer on the ciscoBus controller to reserve for use for the HSSI receiver. When this happens, the HSSI shuts down its receiver and waits until a buffer is available. Data is not lost unless a packet comes in and overflows the HSSI FIFO. Usually, the receive disables are frequent but do not last for long, and the number of dropped packets is less than the count in the “rx disabled” field. A receive disabled condition can happen in systems that are under heavy traffic load and that have shorter packets. In this situation, the number of buffers available on the ciscoBus controller is at a premium. One way to alleviate this problem is to reduce the maximum transmission unit (MTU) on the HSSI interface from 4500 (FDDI size) to 1500 (Ethernet size). Doing so allows the software to take the fixed memory of the ciscoBus controller and divide it into a larger number of smaller buffers, rather than a small number of large buffers. Receive disables are not errors, so they are not included in any error counts.

Field	Description
input errors	Sum of all errors that prevented the receipt of datagrams on the interface being examined. This may not balance with the sum of the enumerated output errors, because some datagrams may have more than one error and others may have errors that do not fall into any of the specifically tabulated categories.
CRC	Cyclic redundancy checksum (CRC) generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data. On a serial link CRCs usually indicate noise, gain hits, or other transmission problems on the data link. CRC errors are also reported when a far-end abort occurs, and when the idle flag pattern is corrupted. This makes it possible to get CRC errors even when there is no data traffic.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a serial line, this is usually the result of noise or other transmission problems.
overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the ability of the receiver to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be increased.
abort	Number of packets whose receipt was aborted.
packets output	Total number of messages transmitted by the system.
bytes output	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the far-end transmitter has been running faster than the near-end router receiver can handle.
congestion drop	Number of messages discarded because the output queue on an interface grew too long. This can happen on a slow, congested serial link.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors, because some datagrams may have more than one error, and others may have errors that do not fall into any of the specifically tabulated categories.
applique	Indicates that an unrecoverable error has occurred on the High-System Availability (HSA) applique. The system then invokes an interface reset.

Field	Description
interface resets	Number of times that an interface has been completely reset. This can happen if packets queued for transmission were not sent within several seconds time. On a serial line, this can be caused by a malfunctioning modem that is not supplying the transmit clock signal or by a cable problem. If the system notices that the carrier detect line of a serial interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an interface is looped back or shut down.
restarts	Number of times that the controller was restarted because of errors.
carrier transitions	Number of times that the carrier detect signal of the interface has changed state. Indicates modem or line problems if the carrier detect line is changing state often.

The following is sample output from the **showinterfaceshssi** command on a Cisco 7500 series router:

```
Router# show interfaces hssi 1/0
Hssi1/0 is up, line protocol is up
  Hardware is cxBus HSSI
  Internet address is 10.108.38.14, subnet mask is 255.255.255.0
  MTU 1500 bytes, BW 45045 Kbit, DLY 1000000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input 0:00:00, output 0:00:08, output hang never
  Last clearing of "show interface" counters never
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  Five minute input rate 1000 bits/sec, 2 packets/sec
  Five minute output rate 0 bits/sec, 0 packets/sec
     630573548 packets input, 2077237628 bytes, 0 no buffer
     Received 2832063 broadcasts, 0 runts, 0 giants
              0 parity, 1970 rx disabled
     113 input errors, 20 CRC, 93 frame, 0 overrun, 0 ignored, 0 abort
     629721628 packets output, 1934313295 bytes, 0 underruns
     0 output errors, 0 applique, 62 interface resets, 0 restarts
     309 carrier transitions
```

The following is sample output from the **showinterfaceshssi** command with the **accounting** option on a Cisco 7500 series router:

```
Router# show interfaces hssi 1/0 accounting
HIP1/0
       Protocol    Pkts In   Chars In   Pkts Out  Chars Out
             IP       7344    4787842       1803    1535774
      Appletalk      33345    4797459      12781    1089695
        DEC MOP          0          0        127       9779
            ARP          7        420         39       2340
```

The table below describes thefields shown in the display.

*Table 136: **show interfaces hssi** Field Descriptions--Accounting*

Field	Description
Protocol	Protocol that is operating on the interface.
Pkts In	Number of packets received for that protocol.
Chars In	Number of characters received for that protocol.

Field	Description
Pkts Out	Number of packets transmitted for that protocol.
Chars Out	Number of characters transmitted for that protocol.

show interfaces integrated-service-engine

To show the Cisco wireless LAN controller network module (WLCM) interfaces on the router, use the **showinterfacesintegrated-service-engine** command in privileged EXEC mode.

show interfaces integrated-service-engine slot/**unit** {**aaa** | **accounting** | **counters** | **crb** | **dampening** | **description** | **etherchannel** | **irb** | **mac-accounting** | **mpls-exp** | **precedence** | **pruning** | **rate-limit** | **stats** | **status** | **summary** | **switching** | **switchport** | **trunk**}

Syntax Description

slot/unit	Specifies the router slot and unit numbers.
aaa	Shows the dot11 aaa information.
accounting	Shows the interface accounting information.
counters	Shows the interface counters.
crb	Shows the interface routing and bridging information.
dampening	Shows the interface dampening information.
description	Shows the interface description.
etherchannel	Shows the interface Ethernet channel information.
irb	Shows the interface routing and bridging information.
mac-accounting	Shows the interface MAC accounting information.
mpls-exp	Shows the interface MPLS experimental accounting information.
precedence	Shows the interface precedence accounting information.
pruning	Shows the interface trunk VTP pruning information.
rate-limit	Shows the interface rate-limit information.
stats	Shows the interface in and out packets and octets by switching path.
status	Shows the interface line status.
summary	Shows the interface summary.
switching	Shows the interface switching.
switchport	Shows the interface switchport information.
trunk	Shows the interface trunk information.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(15)T	This command was introduced.

Examples

The following example shows how to read the interface information about the WLCM in the router:

```
Router# show interfaces integrated-service-engine
 1/0
integrated-service-engine 1/0 is up, line protocol is up
  Hardware is I82559FE, address is 0005.9a3d.7450 (bia 0005.9a3d.7450)
  Internet address is 30.0.0.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID  1., loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:05, output 00:00:03, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     2400779 packets input, 143127299 bytes
     Received 2349587 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     468232 packets output, 106333102 bytes, 0 underruns
     0 output errors, 0 collisions, 3 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 1 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Related Commands

interface integrated-service-engine

show interfaces ism

To display status, traffic data, and configuration information about the internal service module (ISM) interface, use the **showinterfacesism** command in user EXEC or privileged EXEC mode.

show interfaces ism *slot*/*port*

Syntax Description

slot	Router slot in which the service module is installed. For internal service modules, always use 0.
/ *port*	Port number of the module interface. The slash mark (/) is required.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

The ISM interface is the Gigabit Ethernet interface on the router that connects to the ISM.

Examples

The following example displays status, traffic data, and configuration information about the interface to the ISM installed in the router.

```
Router# show interfaces ism 0/0
ISM0/0 is up, line protocol is up
  Hardware is PSE2, address is 001e.4a97.646d (bia 001e.4a97.646d)
  Internet address is 20.0.0.1/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s, media type is internal
  output flow-control is XON, input flow-control is XON
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:11, output 00:00:11, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/60 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     329 packets input, 34641 bytes, 0 no buffer
     Received 109 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     241 packets output, 79646 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

The table below describes the significant fields shown in the display.

Table 137: show interfaces ism Field Descriptions

Field	Description
Hardware, address	Hardware type and address.
MTU	Maximum transmission unit (MTU) of the service module interface.
BW	Bandwidth of the interface, in kbps.
DLY	Delay of the interface, in microseconds.
reliability	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
txload	Transmit load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
rxload	Receive load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method assigned to the interface.
loopback	Indicates whether or not loopback is set.
Keepalive	Indicates whether or not keepalives are set and the interval between keepalives if they have been set.
ARP type...ARP Timeout	Type of Address Resolution Protocol (ARP) assigned and length of timeout.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by the interface and processed locally on the router. This field is useful for detecting when a dead interface failed. **Note** This field is not updated by fast-switched traffic.
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by the interface. This field is useful for detecting when a dead interface failed.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because a transmission took too long. When the number of hours in any of the “last” fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. Asterisks (***) indicate that the elapsed time is too large to be displayed.

Field	Description
Input queue	Number of packets in the input queue. Each number is followed by a slash, the maximum size of the queue, the number of packets dropped because of a full queue, and the number of times that queued packets have been discarded.
Total output drops	Number of packets in the output queue that have been dropped because of a full queue.
Queueing strategy	Queueing strategy applied to the interface, which is configurable under the interface. The default is FIFO (first-in, first-out).
Output queue	Number of packets in the output queue, and the maximum size of the queue. Each number is followed by a slash.
5 minute input rate, 5 minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic that it sends and receives (rather than all network traffic). The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within 2 percent of the instantaneous rate of a uniform stream of traffic over that period. **Note** The 5-minute period referenced in this output is a load interval that is configurable under the interface. The default value is 5 minutes.
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernets and bursts of noise on serial lines are often responsible for no input buffer events.
Received...broadcasts	Number of broadcasts received.
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium. For instance, any Ethernet packet that is less than 64 bytes is considered a runt.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium. For example, any Ethernet packet that is greater than 1518 bytes is considered a giant.
throttles	Number of times that the interface requested another interface within the router to slow down.

Field	Description
input errors	Errors that include runts, giants, no buffer, cyclic redundancy checksum (CRC), frame, overrun, and ignored counts. Other input-related errors can also cause the input errors count to be increased, and some datagrams may have more than one error; therefore, this sum may not balance with the sum of enumerated input error counts.
CRC	Errors created when the CRC generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station that is transmitting bad data.
frame	Number of packets received incorrectly that have a CRC error and a noninteger number of octets. On a LAN, this is usually the result of collisions or a malfunctioning Ethernet device.
overrun	Number of times that the receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets that were ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different from system buffer space described. Broadcast storms and bursts of noise can cause the ignored count to increase.
input packets with dribble condition detected	Number of packets with dribble condition. Dribble bit error indicates that a frame is slightly too long. This frame error counter is incremented just for informational purposes; the router accepts the frame.
packets output	Total number of messages that have been transmitted by the system.
bytes	Total number of bytes, including data and MAC encapsulation, that have been transmitted by the system.
underruns	Number of times that the transmitter has run faster than the router could handle. This may never be reported on some interfaces.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface that is being examined. Note that this may not balance with the sum of the enumerated output errors, because some datagrams may have more than one error, and others may have errors that do not fall into any of the specifically tabulated categories.
collisions	Number of messages that have been retransmitted because of an Ethernet collision. This is usually the result of an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). A packet that collides is counted only once in output packets.

Field	Description
interface resets	Number of times an interface has been completely reset. This can happen if packets that were queued for transmission were not sent within several seconds. On a serial line, this can be caused by a malfunctioning modem that is not supplying the transmit clock signal or by a cable problem. If the system notices that the carrier detect line of a serial interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an interface is looped back or shut down.
babbles	Count of frames greater than 1518 bytes that have been transmitted, indicating that the transmitter has been on the interface longer than the time necessary to transmit the largest frame.
late collision	Number of late collisions. A collision becomes a late collision when it occurs after the preamble has been transmitted.
deferred	Deferred indicates that the chip, while ready to transmit a frame, had to defer because the carrier was asserted.
lost carrier	Number of times that the carrier was lost during transmission.
no carrier	Number of times that the carrier was not present during the transmission.
output buffer failures, output buffers swapped out	Number of failed buffers and number of buffers swapped out.

Related Commands

Command	Description
show controllers ism	Displays controller information for the service module interface.

show interfaces lex

To display statistics about a LAN Extender interface, use the **showinterfaceslex** command in EXEC mode.

show interfaces lex commandshow interfaces lex *number* [{**ethernet** | **serial**}]

Syntax Description

number	Number of the LAN Extender interface that resides on the core router about which to display statistics.
ethernet	(Optional) Displays statistics about the Ethernet interface that resides on the LAN Extender chassis.
serial	(Optional) Displays statistics about the serial interface that resides on the LAN Extender chassis.

Command Modes

EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(15)T	This command is no longer supported in Cisco IOS Mainline or Technology-based releases. It may conintue to appear in Cisco IOS 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

To display statistics about the LAN Extender interface on the core router, use the **showinterfaceslex** command without any keywords.

Administratively, the physical serial interface that connects the core router to the LAN Extender is completely hidden. The **showinterfacesserial**command will show only that the serial interface is present. However, it will not report any statistics about the traffic passing over the physical line. All statistics are report by the **showinterfaceslex** command.

Examples

The following is sample output from the **showinterfaceslex** command, showing the LAN Extender interface on the host router. Note the “Bound to ...” field, which is displayed only on a LAN Extender interface.

```
Router# show interfaces lex 0
Lex0 is up, line protocol is up
  Hardware is Lan Extender, address is 0204.0301.1526 (bia 0000.0000.0000)
  MTU 1500 bytes, BW 10000 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 4:00:00
  Bound to Serial3
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  Five minute input rate 1000 bits/sec, 0 packets/sec
```

```
  Five minute output rate 0 bits/sec, 0 packets/sec
     1022 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     2070 packets output, 23663 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets, 0 restarts
```

The following is sample output from the **showinterfaceslex** command when you specify the **ethernet** keyword:

```
Router# show interfaces lex 0 ethernet
Lex0-Ethernet0 is up, line protocol is up
  Hardware is LAN-Extender, address is 0000.0c01.1526 (bia 0000.0c01.1526)
  Last input 6w3d, output 6w3d
  Last clearing of "show interface" counters 0:02:30
  Output queue 40/50, 60 drops; input queue 10/40, 2 drops
  Five minute input rate 0 bits/sec, 0 packets/sec
  Five minute output rate 0 bits/sec, 0 packets/sec
     3916 packets input, 960303 bytes, 3 no buffer
     Received 2 broadcasts, 3 runts, 3 giants
     2 input errors, 1 CRC, 1 frame, 1 overrun, 3 ignored, 2 abort
     2500 packets output, 128288 bytes, 1 underruns
     1 output errors, 1 collisions, 0 interface resets, 0 restarts
```

The following is sample output from the **showinterfaceslex** command when you specify the **serial** keyword:

```
Router# show interfaces lex 0 serial
Lex0-Serial0 is up, line protocol is up
  Hardware is LAN-Extender
  Last input 6w3d, output 6w3d
  Last clearing of "show interface" counters 0:03:05
  Input queue: 5/15/4 (size/max/drops); Total output drops: 450
  Output queue: high 25/35/90, medium 70/80/180, normal 40/50/120, low 10/20/60
  Five minute input rate 0 bits/sec, 0 packets/sec
  Five minute output rate 0 bits/sec, 0 packets/sec
     1939 packets input, 30998 bytes, 6 no buffer
     Received 4 broadcasts, 6 runts, 6 giants
     4 input errors, 2 CRC, 2 frame, 2 overrun, 6 ignored, 4 abort
     1939 packets output, 219535 bytes, 2 underruns
     2 output errors, 2 collisions, 0 interface resets, 0 restarts
     2 carrier transitions
```

The table below describes the fields shown in the preceding displays.

Table 138: show interfaces lex Field Descriptions

Field	Description
Lex0 is up, line protocol is up	Indicates whether the logical LAN Extender interface on the core router is currently active (that is, whether carrier detect is present), inactive, or has been taken down by an administrator.
Lex0-Ethernet0 is up, line protocol is up Lex0-Serial0 is up, line protocol is up	Indicates whether the physical Ethernet and serial interfaces on the LAN Extender chassis are currently active (that is, whether carrier detect is present) and whether it has been taken down by an administrator.
Hardware is LAN-Extender	Hardware type of the interfaces on the LAN Extender.

Field	Description
address is ...	Logical MAC address of the interface.
bia	Burned-in MAC address of the interface. The LAN Extender interface does not have a burned in address; hence it appears as all zeroes.
MTU	Maximum transmission unit size of the interface.
BW	Value of the bandwidth parameter that has been configured for the interface (in kilobits per second). The bandwidth parameter is used to compute IGRP metrics only. If the interface is attached to a serial line with a line speed that does not match the default (1536 or 1544 for T1 and 56 for a standard synchronous serial line), use the **bandwidth** command to specify the correct line speed for this serial line.
DLY	Delay of the interface in microseconds.
rely	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method assigned to interface.
ARP type	Type of Address Resolution Protocol assigned.
ARP Timeout	Number of hours, minutes, and seconds an ARP cache entry will stay in the cache.
Bound to ...	Number of the serial interface to which the logical LAN Extender interface is bound.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This counter is updated only when packets are process switched, not when packets are fast switched.
output	Number of hours, minutes, and seconds (or never) since the last packet was successfully transmitted by an interface. This counter is updated only when packets are process switched, not when packets are fast switched.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the “last” fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.

Field	Description
Last clearing of "show interface" counters	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. *** indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 231 ms (and less than 232 ms) ago.
Output queue, drops input queue, drops	Number of packets in output and input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped because of a full queue.
Five minute input rate Five minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes. The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernet networks and bursts of noise on serial lines are often responsible for no input buffer events.
Received ... broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium.
input errors	Total number of no buffer, runts, giants, CRCs, frame, overrun, ignored, and abort counts. Other input-related errors can also increment the count, so that this sum might not balance with the other counts.
CRC	Cyclic redundancy checksum generated by the originating station or far-end device does not match the checksum calculated from the data received. On a serial link, CRCs usually indicate noise, gain hits, or other transmission problems on the data link.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a serial line, this is usually the result of noise or other transmission problems.

Field	Description
overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. Broadcast storms and bursts of noise can cause the ignored count to be increased.
abort	Illegal sequence of one bits on a serial interface. This usually indicates a clocking problem between the serial interface and the data link equipment.
input packets with dribble condition detected	Does not apply to a LAN Extender interface.
packets output	Total number of messages transmitted by the system.
bytes	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the transmitter has been running faster than the router can handle. This might never be reported on some interfaces.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this might not balance with the sum of the enumerated output errors, as some datagrams may have more than one error, and others may have errors that do not fall into any of the specifically tabulated categories.
collisions	Number of messages retransmitted because of an Ethernet collision. Some collisions are normal. However, if your collision rate climbs to around 4 or 5 percent, you should consider verifying that there is no faulty equipment on the segment and/or moving some existing stations to a new segment. A packet that collides is counted only once in output packets.
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within several seconds' time. On a serial line, this can be caused by a malfunctioning modem that is not supplying the transmit clock signal, or by a cable problem. If the system notices that the carrier detect line of a serial interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an interface is looped back or shut down.
restarts	Number of times the controller was restarted because of errors.

show interfaces loopback

To display information about the loopback interface, use the **showinterfacesloopback**command in privileged EXEC mode.

show interfaces loopback commandshow interfaces loopback [*number*] [**accounting**]

Syntax Description

number	(Optional) Port number on the selected interface.
accounting	(Optional) Displays the number of packets of each protocol type that have been sent through the interface.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **showinterfacesloopback** command:

```
Router# show interfaces loopback 0
Loopback0 is up, line protocol is up
  Hardware is Loopback
  MTU 1500 bytes, BW 1 Kbit, DLY 50 usec, rely 255/255, load 1/255
  Encapsulation UNKNOWN, loopback not set, keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Output queue 0/0, 0 drops; input queue 0/75, 0 drops
  Five minute input rate 0 bits/sec, 0 packets/sec
  Five minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets, 0 restarts
```

The following is sample output when the **accounting** keyword is included:

```
Router# show interfaces loopback 0 accounting
Loopback0
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
No traffic sent or received on this interface.
```

The table below describes significant fields shown in the displays.

*Table 139: **show interfaces loopback** Field Descriptions*

Field	Description
Loopback is {up | down | administratively down}	Indicates whether the interface hardware is currently active (whether carrier detect is present), is currently inactive, or has been taken down by an administrator.
line protocol is {up | down | administratively down}	Indicates whether the software processes that handle the line protocol consider the line usable (that is, whether keepalives are successful).
Hardware	Hardware is Loopback.
MTU	Maximum transmission unit of the interface.
BW	Bandwidth of the interface, in kilobits per second.
DLY	Delay of the interface, in microseconds.
rely	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method assigned to interface.
loopback	Indicates whether loopback is set and type of loopback test.
keepalive	Indicates whether keepalives are set or not.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This counter is updated only when packets are process-switched, not when packets are fast-switched.
Last output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by an interface. This counter is updated only when packets are process-switched, not when packets are fast-switched.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the “last” fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. *** indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 231 ms (and less than 232 ms) ago.

Field	Description
Output queue, drops; Input queue, drops	Number of packets in output and input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped because of a full queue.
Five minute input rate, Five minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes.
packets input	Total number of error-free packets received by the system.
bytes input	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernet networks and bursts of noise on serial lines are often responsible for no input buffer events.
broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium.
input errors	Sum of all errors that prevented the receipt of datagrams on the interface being examined. This may not balance with the sum of the enumerated output errors, because some datagrams may have more than one error and others may have errors that do not fall into any of the specifically tabulated categories.
CRC	Cyclic redundancy checksum generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data. On a serial link, CRCs usually indicate noise, gain hits, or other transmission problems on the data link. CRC errors are also reported when a far-end abort occurs, and when the idle flag pattern is corrupted. This makes it possible to get CRC errors even when there is no data traffic.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a serial line, this is usually the result of noise or other transmission problems.
overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be increased.
abort	Number of packets whose receipt was aborted.

Field	Description
packets output	Total number of messages transmitted by the system.
bytes output	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the far-end transmitter has been running faster than the near-end router's receiver can handle. This may never happen (be reported) on some interfaces.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors, as some datagrams may have more than one error, and others may have errors that do not fall into any of the specifically tabulated categories.
collisions	Loopback interface does not have collisions.
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within several seconds time. On a serial line, this can be caused by a malfunctioning modem that is not supplying the transmit clock signal, or by a cable problem. If the system notices that the carrier detect line of a serial interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an interface is looped back or shut down.
restarts	Number of times the controller was restarted because of errors.
Protocol	Protocol that is operating on the interface.
Pkts In	Number of packets received for that protocol.
Chars In	Number of characters received for that protocol.
Pkts Out	Number of packets transmitted for that protocol.
Chars Out	Number of characters transmitted for that protocol.

show interfaces port-channel

To display the information about the Fast EtherChannel on Cisco 7000 series routers with the RSP7000 and RSP7000CI, Cisco 7200 series routers, and Cisco 7500 series routers, use the **showinterfacesport-channel** command in user EXEC or privileged EXEC mode.

show interfaces port-channel commandshow interfaces port-channel [*channel-number*]

Syntax Description

channel-number	(Optional) Port channel number. Range is from 1 to 4.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
11.1 CA	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.2(02)SA	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Examples

The following is sample output from the **showinterfacesport-channel** command:

Note By default the hardware type is set to Fast EtherChannel.The default MTU is set to 1500 bytes. The maximum MTU size that can be configured on the native Gigabit Ethernet ports on the Cisco 7200 series router is 9216. The range of configurable MTU value is from 1500 to 9216.

```
Router# show interfaces port-channel 1
Port-channel1 is up, line protocol is up
  Hardware is FEChannel, address is 0000.0ca8.6220 (bia 0000.0000.0000)
  MTU 1500 bytes, BW 400000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive not set, fdx
  ARP type: ARPA, ARP Timeout 04:00:00
    No. of active members in this channel: 4
        Member 0 : Fast Ethernet1/0/0
        Member 1 : Fast Ethernet1/1/0
        Member 2 : Fast Ethernet4/0/0
        Member 3 : Fast Ethernet4/1/0
  Last input 01:22:13, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     223 packets input, 11462 bytes, 0 no buffer
     Received 1 broadcasts, 0 runts, 0 giants
```

```
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast
     0 input packets with dribble condition detected
     192 packets output, 13232 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

The following sample output from the **showinterfacesport-channel** shows Gigabit EtherChannel as hardware type and the MTU value as 9216:

```
Router# show interface port-channel 1
Port-channel1 is up, line protocol is up
  Hardware is GEChannel
, address is 0001.c929.c41b (bia 0001.c929.c41b)
  MTU 9216 bytes
, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Unknown duplex, Unknown Speed, media type is unknown media type
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
    No. of active members in this channel: 1
        Member 0 : GigabitEthernet0/1 , Full-duplex, 1000Mb/s
    No. of Non-active members in this channel: 0
  Last input 00:00:04, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     95 packets input, 34383 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     1 packets output, 77 bytes, 0 underruns
     2 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

The table below describes significant fields shown in the display.

*Table 140: **show interfaces port-channel** Field Descriptions*

Field	Description
Port-channel1 is up, line protocol is up	Indicates if the interface hardware is currently active and can transmit and receive or if it has been taken down by an administrator.
Hardware is	Hardware type (Fast EtherChannel).
address is	Address being used by the interface.
MTU	Maximum transmission unit of the interface.
BW	Bandwidth of the interface, in kilobits per second.

Field	Description
DLY	Delay of the interface, in microseconds.
rely	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes. The calculation uses the value from the **bandwidth** interface configuration command.
Encapsulation	Encapsulation method assigned to the interface.
loopback	Indicates if loopbacks are set.
keepalive	Indicates if keepalives are set.
fdx	Indicates the interface is operating in full-duplex mode.
ARA type	ARP type on the interface.
ARP timeout	Number of hours, minutes, and seconds an ARP cache entry will stay in the cache.
No. of active members in this channel: 4	Number of Fast Ethernet interfaces that are currently active (not down) and part of the Fast EtherChannel group.
Member 0: Fast Ethernet1/0/0	Specific Fast Ethernet interface that is part of the Fast EtherChannel group.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This counter is updated only when packets are process-switched, not when packets are fast-switched.
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by an interface. This counter is updated only when packets are process-switched, not when packets are fast-switched.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the “last” fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.
last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. *** indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 231 ms (and less than 232 ms)) ago.

Field	Description
Queueing strategy	First-in, first-out queueing strategy (other queueing strategies you might see are priority-list, custom-list, and weighted fair).
Output queue, drops input queue, drops	Number of packets in output and input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped because a queue was full.
5 minute input rate 5 minute output rate	Average number of bits and packets received or transmitted per second in the last 5 minutes.
packets input	Total number of error-free packets received by the system.
bytes (input)	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernets and bursts of noise on serial lines are often responsible for no input buffer events.
broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium.
input errors	Total number of no buffer, runts, giants, CRCs, frame, overrun, ignored, and abort counts. Other input-related errors can also increment the count, so that this sum might not balance with the other counts.
CRC	Cyclic redundancy checksum generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data. On a serial link, CRCs usually indicate noise, gain hits or other transmission problems on the data link.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a serial line, this is usually the result of noise or other transmission problems.
overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be incremented.
abort	Illegal sequence of ones bit on the interface.

Field	Description
watchdog	Number of times watchdog receive timer expired. It happens when receiving a packet with length greater than 2048.
multicast	Number of multicast packets received.
input packets with dribble condition detected	Dribble bit error indicates that a frame is slightly too long. This frame error counter is incremented just for informational purposes; the router accepts the frame.
packets output	Total number of messages transmitted by the system.
bytes (output)	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the far-end transmitter has been running faster than the near-end router's receiver can handle.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this might not balance with the sum of the enumerated output errors, as some datagrams can have more than one error, and others can have errors that do not fall into any of the specifically tabulated categories.
collisions	Number of messages retransmitted because of an Ethernet collision. A packet that collides is counted only once in output packets.
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within a certain interval. If the system notices that the carrier detect line of an interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an unrecoverable interface processor error occurred, or when an interface is looped back or shut down.
babbles	The transmit jabber timer expired.
late collision	Number of late collisions. Late collision happens when a collision occurs after transmitting the preamble. The most common cause of late collisions is that your Ethernet cable segments are too long for the speed at which you are transmitting.
deferred	Deferred indicates that the chip had to defer while ready to transmit a frame because the carrier was asserted.
lost carrier	Number of times the carrier was lost during transmission.
no carrier	Number of times the carrier was not present during the transmission.
output buffer failures	Number of times that a packet was not output from the output hold queue because of a shortage of MEMD shared memory.
output buffers swapped out	Number of packets stored in main memory when the output queue is full; swapping buffers to main memory prevents packets from being dropped when output is congested. The number is high when traffic is bursty.

Related Commands

Command	Description
interface multilink	Specifies a Fast EtherChannel and enters interface configuration mode.

show interfaces port-channel etherchannel

To display the load-balancing bucket distribution currently in use for a Gigabit EtherChannel (GEC) interface, use the **showinterfacesport-channeletherchannel** command in user EXEC or privileged EXEC mode.

show interfaces port-channel *channel-number* **etherchannel**

Syntax Description

channel-number	Port-channel group number. Range: 1 to 64.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. Information about flow-based load balancing was added to the output.

Usage Guidelines

The **showinterfacesport-channeletherchannel** command shows the bucket-to-member link mappings for load balancing on the GEC interface.

Load balancing uses the concept of buckets to map traffic flows to the member links of a port channel. The different traffic flows are mapped to buckets and each bucket has one active member link associated with it. All traffic flows that are mapped to a bucket use the member link assigned to the bucket.

There are two methods of load balancing on a GEC interface:

- VLAN-manual--All packets forwarded over the same VLAN subinterface are considered part of the same flow and are mapped to the member link specified in the configuration.
- Flow-based--Traffic flows are mapped to different member links based on the packet header.

Examples

The following example shows output from this command for a port channel with VLAN-manual load balancing configured:

```
Router# show interfaces port-channel 2 etherchannel

 All IDBs List contains 3 configured interfaces
  Port: GigabitEthernet2/1/6 (index: 0)
  Port: GigabitEthernet2/1/7 (index: 1)
  Port: GigabitEthernet2/1/0 (index: 2)

 Active Member List contains 1 interfaces
  Port: GigabitEthernet2/1/0

 Passive Member List contains 2 interfaces
  Port: GigabitEthernet2/1/6
    VLAN 1 (Pri, Ac, D, P)    VLAN 50 (Sec, St, D, P)
  Port: GigabitEthernet2/1/7
    VLAN 1 (Sec, St, D, P)    VLAN 50 (Pri, Ac, C, P)
 Load-Balancing method applied: vlan-manual

 Bucket Information for VLAN Manual LB:
```

```
   Bucket 0   (p=GigabitEthernet2/1/6, s=GigabitEthernet2/1/6) active GigabitEthernet2/1/6

   Bucket 1   (p=GigabitEthernet2/1/6, s=GigabitEthernet2/1/7) active GigabitEthernet2/1/6

   Bucket 2   (p=GigabitEthernet2/1/6, s=GigabitEthernet2/1/0) active GigabitEthernet2/1/0

   Bucket 4   (p=GigabitEthernet2/1/7, s=GigabitEthernet2/1/6) active GigabitEthernet2/1/7

   Bucket 5   (p=GigabitEthernet2/1/7, s=GigabitEthernet2/1/7) active GigabitEthernet2/1/7

   Bucket 6   (p=GigabitEthernet2/1/7, s=GigabitEthernet2/1/0) active GigabitEthernet2/1/0

   Bucket 8   (p=GigabitEthernet2/1/0, s=GigabitEthernet2/1/6) active GigabitEthernet2/1/0

   Bucket 9   (p=GigabitEthernet2/1/0, s=GigabitEthernet2/1/7) active GigabitEthernet2/1/0

   Bucket 10   (p=GigabitEthernet2/1/0, s=GigabitEthernet2/1/0) active GigabitEthernet2/1/0
```

The following example shows output for a port channel with flow-based load balancing configured:

```
Router(config)# show interfaces port-channel 2 etherchannel

 All IDBs List contains 3 configured interfaces
  Port: GigabitEthernet2/1/6 (index: 0)
  Port: GigabitEthernet2/1/7 (index: 1)
  Port: GigabitEthernet2/1/0 (index: 2)

 Active Member List contains 1 interfaces
  Port: GigabitEthernet2/1/0

 Passive Member List contains 2 interfaces
  Port: GigabitEthernet2/1/6

  Port: GigabitEthernet2/1/7

 Load-Balancing method applied: flow-based

 Bucket Information for Flow-Based LB:
 Interface:                                Buckets
    GigabitEthernet2/1/0:
                          Bucket 0 , Bucket 1 , Bucket 2 , Bucket 3
                          Bucket 4 , Bucket 5 , Bucket 6 , Bucket 7
                          Bucket 8 , Bucket 9 , Bucket 10, Bucket 11
                          Bucket 12, Bucket 13, Bucket 14, Bucket 15
```

The table below describes the significant fields shown in the display.

Table 141: show interfaces port-channel etherchannel Field Descriptions

Field	Description
Active Member List	List of active physical interfaces in the GEC bundle.
Passive Member List	List of passive (backup) physical interfaces in the GEC bundle.
Load-Balancing method applied	The load-balancing method configured on the interface, either flow-based or vlan-manual.
Bucket Information	Lists the bucket information across the active member links.

Related Commands

Command	Description
load-balancing	Applies a load-balancing method to a GEC interface.
port-channel load-balancing vlan-manual	Applies the VLAN-manual load-balancing method globally to all GEC interfaces.
show etherchannel load-balancing	Displays the load-balancing method applied to GEC interfaces.

show interfaces pos

To display configuration information and statistics for a Packet over SONET (POS) interface, use the **showinterfacespos** command in user EXEC or privileged EXEC configuration mode.

Cisco 7000 and Cisco 7500 Series with VIPs
show interfaces pos commandshow interfaces pos [*slot* / *port-adapter* / *port*]

POS Shared Port Adapters
show interfaces pos [*slot* / *subslot* / *port* [/ *sub_int*]]

Syntax Description

slot / *port-adapter* / *port*	**(Optional) Cisco 7000 or Cisco 7500 Series Routers** Number of the chassis slot that contains the POS interface (for example, 2/0/0), where: • *slot* --Chassis slot number. • / *port-adapter*-- Port adapter number. • / *port*-- Port or interface number. Refer to the appropriate hardware manual for slot and port information, and port adapter compatibility.
slot / *subslot* / *port* / *sub_int*	**(Optional) POS Shared Port Adapters** Number of the chassis slot that contains the POS interface (for example 4/3/0), where: • *slot* --Chassis slot number. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide. • / *subslot*-- Secondary slot number on a SPA interface processor (SIP) where a SPA is installed. Refer to the platform-specific SPA hardware installation guide and the corresponding "Specifying the Interface Address on a SPA" topic in the platform-specific SPA software configuration guide for subslot information. • / *port* --Port or interface number. For SPAs, refer to the corresponding "Specifying the Interface Address on a SPA" topics in the platform-specific SPA software configuration guide. • / *sub_int* -- (Optional) Subinterface number.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
11.2	The **showinterfaceposi** command was introduced.
11.3	The name of the command was modified from **showinterfaceposi**to **showinterfacespos**, and the sample output was updated.
12.2(25)S3	This command was integrated into Cisco IOS Release 12.2(25)S3 to support SPAs on the Cisco 7304 router. The command was modified to support a new addressing format for SPAs.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE to support SPAs on the Cisco 7600 series routers and Catalyst 6500 series switches.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S to support SPAs on the Cisco 12000 series routers.

Examples

Cisco 7513 Example

The following is sample output from the **showinterfacespos** command on a Cisco 7513 router with one Packet OC-3 Interface Processor (POSIP):

```
Router# show interfaces pos 2/0/0
POS2/0/0 is up, line protocol is up
  Hardware is cyBus Packet over Sonet
  Description: PRI-T1 net to zippy (4K) to Pac-Bell
  Internet address is 10.1.1.1/27
  MTU 4470 bytes, BW 1000 Kbit, DLY 40000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (3 sec)
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters 00:23:09
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 1 packets/sec
  5 minute output rate 1000 bits/sec, 1 packets/sec
     1046 packets input, 54437 bytes, 0 no buffer
     Received 485 broadcasts, 0 runts, 0 giants, 0 parity
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     4013 packets output, 1357412 bytes, 0 underruns
     0 output errors, 0 applique, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
```

Cisco 7600 Series Router and Catalyst 6500 Series Switch POS Shared Port Adapter Example

The following is sample output from the **showinterfacespos** command on a Cisco 7600 series router or Catalyst 6500 series switch for POS interface 4/3/0 (which is the interface for port 0 of the SPA in subslot 3 of the SIP in chassis slot 4):

```
Router# show interfaces pos 4/3/0

POS4/3/0 is up, line protocol is up  (APS working - active)
  Hardware is Packet over SONET
  Internet address is 10.0.0.1/8
  MTU 4470 bytes, BW 622000 Kbit, DLY 100 usec, rely 255/255, load 1/255
```

```
  Encapsulation HDLC, crc 16, loopback not set
  Keepalive not set
  Scramble disabled
  Last input 00:00:34, output 04:09:06, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy:fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
        Available Bandwidth 622000 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     782 packets input, 226563 bytes, 0 no buffer
     Received 0 broadcasts, 1 runts, 0 giants, 0 throttles
              0 parity
     1 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     271 packets output, 28140 bytes, 0 underruns
     0 output errors, 0 applique, 2 interface resets
     0 output buffer failures, 0 output buffers swapped out
     2 carrier transitions
```

Cisco 12000 Series Router POS Shared Port Adapter Example

The following is sample output from the **showinterfacespos** command on a Cisco 12000 series router for POS interface 1/1/0 (which is the interface for port 0 of the SPA in subslot 1 of the SIP in chassis slot 1):

```
Router# show interfaces pos 1/1/0

POS1/1/0 is up, line protocol is up
  Hardware is Packet over SONET
  Internet address is 10.41.41.2/24
  MTU 4470 bytes, BW 9952000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation HDLC, crc 32, loopback not set
  Keepalive not set
  Scramble enabled
  Last input 00:00:59, output 00:00:11, output hang never
  Last clearing of "show interface" counters 00:00:14
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
        Available Bandwidth 9582482 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
              0 parity
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     1 packets output, 314 bytes, 0 underruns
     0 output errors, 0 applique, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
```

The table below describes the significant fields shown in these displays.

*Table 142: **show interfaces pos** Field Descriptions*

Field	Description
POSx/y/z is up, line protocol is up	Indicates whether the interface hardware is currently active and can transmit and receive or whether it has been taken down by an administrator.

Field	Description
Hardware is. . .	Hardware type: • For POSIP-- cyBus Packet over Sonet • For POS SPAs--Packet over SONET
Internet address is	Internet address and subnet mask.
MTU	Maximum transmission unit of the interface.
BW	Bandwidth of the interface, in kilobits per second.
DLY	Delay of the interface, in microseconds.
rely	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes. The calculation uses the value from the **bandwidth** interface configuration command.
Encapsulation	Encapsulation method assigned to interface.
Loopback	Indicates whether loopbacks are set.
Keepalive	Indicates whether keepalives are set.
Scramble	Indicates whether or not SONET payload scrambling is enabled. SONET scrambling is disabled by default. For the POS SPAs on the Cisco 12000 series routers, scrambling is enabled by default.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This counter is updated only when packets are process-switched, not when packets are fast-switched.
(Last) output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by an interface. This counter is updated only when packets are process-switched, not when packets are fast-switched.
(Last) output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the “last” fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.

Field	Description
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. *** indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 2231 ms (and less than 232 ms) ago.
Queueing strategy	First-in, first-out (FIFO) queueing strategy (other queueing strategies you might see are priority-list, custom-list, and weighted fair).
Output queue, drops input queue, drops	Number of packets in output and input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped because a queue was full.
5 minute input rate 5 minute output rate	Average number of bits and packets received or transmitted per second in the last 5 minutes.
packets input	Total number of error-free packets received by the system.
bytes (input)	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernets and bursts of noise on serial lines are often responsible for no input buffer events.
broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium.
throttles	Not supported for POS interfaces.
parity	Report of the parity errors on the interface.
input errors	Total number of no buffer, runts, giants, CRCs, frame, overrun, ignored, and abort counts. Other input-related errors can also increment the count, so that this sum might not balance with the other counts.
CRC	Cyclic redundancy checksum generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data. On a serial link, CRCs usually indicate noise, gain hits or other transmission problems on the data link.

Field	Description
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a serial line, this is usually the result of noise or other transmission problems.
overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be incremented.
abort	Illegal sequence of one bits on the interface.
packets output	Total number of messages transmitted by the system.
bytes (output)	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the far-end transmitter has been running faster than the near-end router's receiver can handle.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this might not balance with the sum of the enumerated output errors, as some datagrams can have more than one error, and others can have errors that do not fall into any of the specifically tabulated categories.
applique	Indicates an unrecoverable error has occurred on the POSIP applique. The system then invokes an interface reset.
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within a certain interval. If the system notices that the carrier detect line of an interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an unrecoverable interface processor error occurred, or when an interface is looped back or shut down.
output buffer failures	Not supported for POS interfaces.
output buffers swapped out	Not supported for POS interfaces.
carrier transitions	Number of times the carrier detect signal of the interface has changed state.

Related Commands

Command	Description
interface	Configures an interface type and enters interface configuration mode.

show interfaces private-vlan mapping

To display the information about the private virtual local area network (PVLAN) mapping for VLAN SVIs, use the **showinterfacesprivate-vlanmapping** command in user EXEC or privileged EXEC mode.

show interfaces [*interface interface-number*] **private-vlan mapping** [**active**]

Syntax Description

interface	(Optional) Interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **pos**, **atm**, and **ge-wan**.
interface-number	(Optional) Module and port number; see the "Usage Guidelines" section for valid values.
active	(Optional) Displays the active interfaces only.

Command Default

This command has no default settings.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **pos**, **atm**, and **ge-wan** keywords are supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

This command displays SVI information only.

The *interface-number*argument designates the module and port number. Valid values for *interface-number* depend on the chassis and module that are used. For example, if you have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the slot number are from 1 to 13 and valid values for the port number are from 1 to 48.

Examples

This example shows how to display the information about the PVLAN mapping:

```
Router# show interfaces private-vlan mapping
Interface Secondary VLAN Type
--------- -------------- -----------------
vlan2     301            community
vlan2     302            community
Router#
```

Related Commands

Command	Description
private-vlan	Configures PVLANs and the association between a PVLAN and a secondary VLAN.

Command	Description
private-vlan mapping	Creates a mapping between the primary and the secondary VLANs so that both VLANs share the same primary VLAN SVI.

show interfaces satellite

To display general interface settings and traffic rates for the internal router interface that connects to an installed Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT), use the **showinterfacessatellite** command in user EXEC or privileged EXEC mode.

Syntax:

show interfaces satellite *slot* / *unit*

Syntax Description

slot	Router chassis slot in which the network module is installed.
unit	Interface number. For NM-1VSAT-GILAT network modules, always use 0.

Command Default

No default behavior or values.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The **showinterfacessatellite** command shows these items:

- Basic configuration information for the internal router interface that connects to an installed Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT)
- Traffic statistics, including the number of packets transmitted, input and output rate, and errors
- Interface and line protocol status (up or down), with the following exceptions:
    - *Line Protocol Status Exception - Hub Dial Backup Mode*
    - *Line Protocol Status Exception - Hot Standby Router Protocol (HSRP) Standby Mode*

Line Protocol Status Exception--Hub Dial Backup Mode

If you configure hub dial backup mode on the satellite interface, then the **showinterfacessatellite** command always displays Line Protocol Up status, even when the line protocol is down. To view the actual line protocol status, enter the **showcontrollerssatellite** command or the **service-modulesatellite***slot***/0status** command in privileged EXEC mode.

Line Protocol Status Exception--Hot Standby Router Protocol (HSRP) Standby Mode

If the router is in a hot standby group and is in standby mode, then the **showinterfacessatellite** command displays “line protocol is up (standby)”, even though a link to the hub is not established from the standby router. To view the actual line protocol status, enter the **showcontrollerssatellite** command or the **service-modulesatellite***slot***/0status** command in privileged EXEC mode.

Examples

For output field descriptions, see the table below.

This section provides the following examples:

Normal Operation or Hub Dial Backup Mode Example

In the following example, the satellite interface is up and the line protocol is up.

If you configure hub dial backup for the NM-1VSAT-GILAT network module, the line protocol appears to be up even if the satellite link is actually down. To view the actual line protocol status while hub dial backup mode is configured, use the **showcontrollerssatellite** command or the **service-modulesatellite***slot*/**0status** command instead.

```
Router# show interfaces satellite 2/0

Satellite2/0 is up
, line protocol is up
  Hardware is I82559FE, address is 0008.e35f.7370 (bia 0008.e35f.7370)
  Internet address is 10.22.1.2/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not set
  ARP type:ARPA, ARP Timeout 04:00:00
  Last input 00:00:02, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue:0/75/0/0 (size/max/drops/flushes); Total output drops:0
  Queueing strategy:fifo
  Output queue:0/40 (size/max)
  5 minute input rate 13000 bits/sec, 6 packets/sec
  5 minute output rate 8000 bits/sec, 9 packets/sec
     419433 packets input, 108329352 bytes, 0 no buffer
     Received 11792 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     650568 packets output, 73969720 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Satellite Backup for a Terrestrial Link--Standby Mode Example

In the following example, the satellite interface is in standby mode because the primary terrestrial link is up:

```
Router# show interfaces satellite 1/0

Satellite1/0 is standby mode
, line protocol is down

  Hardware is I82559FE, address is 00e0.f7ff.f310 (bia 00e0.f7ff.f310)
  Internet address is 10.0.0.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not set
  ARP type:ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:03, output hang never
  Last clearing of "show interface" counters 00:00:04
  Input queue:0/75/0/0 (size/max/drops/flushes); Total output drops:0
  Queueing strategy:fifo
```

```
  Output queue:0/40 (size/max)
  30 second input rate 13000 bits/sec, 6 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
     30 packets input, 7474 bytes, 0 no buffer
     Received 1 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     1 packets output, 82 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Hot Standby Router Protocol (HSRP)--Standby Mode Example

In the following example, homogeneous HSRP is configured on two routers, each of which contains an NM-1VSAT-GILAT network module that connects to the same dish antenna (ODU). The following output from the standby router shows that the line protocol is "up (standby)," even though the satellite link on the standby router is actually down. To view the actual line protocol status, use the **showcontrollerssatellite** command or the **service-modulesatellite***slot*/**0status** command.

```
Router# show interfaces satellite 2/0

Satellite2/0 is up
, line protocol is up (standby)
  Hardware is I82559FE, address is 0008.e35f.7370 (bia 0008.e35f.7370)
  Internet address is 10.22.1.2/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not set
  ARP type:ARPA, ARP Timeout 04:00:00
  Last input 00:00:02, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue:0/75/0/0 (size/max/drops/flushes); Total output drops:0
  Queueing strategy:fifo
  Output queue:0/40 (size/max)
  5 minute input rate 13000 bits/sec, 6 packets/sec
  5 minute output rate 8000 bits/sec, 9 packets/sec
     419433 packets input, 108329352 bytes, 0 no buffer
     Received 11792 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     650568 packets output, 73969720 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

The table below describes the significant fields shown in the display.

Table 143: show interfaces satellite Field Descriptions

Field	Description
Satellite2/0 is... • up • down • standby mode	State of the interface hardware: • Currently active. • Has been taken down by an administrator. • In HSRP standby mode when two HSRP-redundant NM-1VSAT-GILAT network modules (in separate routers) connect to one dish antenna (ODU).
line protocol is	State of the backbone link to the hub: up or down. See the following exceptions:
Hardware is	Hardware type (for example, Fast Ethernet) and address.
Internet address	Internet address followed by subnet mask.
MTU	Maximum transmission unit of the interface.
BW	Bandwidth of the interface, in kilobits per second.
DLY	Delay of the interface, in microseconds.
reliability	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
txload and rxload	Transmitted and received load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method assigned to the interface.
loopback	Indicates whether loopback is set or not.
keepalive	Indicates whether keepalives are set or not.
ARP type	Type of Address Resolution Protocol assigned.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This counter is updated only when packets are process-switched, not when packets are fast-switched.
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by the interface. Useful for knowing when a dead interface failed. This counter is updated only when packets are process-switched, not when packets are fast-switched.

Field	Description
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. *** indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 2 31 ms (and less than 2 32 ms) ago.
Input queue	Input queue information: • Size--Number of packets in the input queue • Max--Maximum size of the queue • Drops--Number of packets discarded because of a full queue • Flushes--Number of times data on queue has been discarded
Total output drops	Total number of output packets dropped.
Queueing strategy	First-in, first-out queueing strategy (other queueing strategies you might see are priority-list, custom-list, and weighted fair).
Output queue	Number of packets in the output queue and the maximum size of the queue,
5 minute input rate 5 minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes. The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernet networks and bursts of noise on serial lines are often responsible for no input buffer events.
broadcasts	Total number of broadcast or multicast packets received by the interface.

Field	Description
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the media.
giants	Number of packets that are discarded because they exceed the maximum packet size of the media.
throttles	Number of times that the interface requested another interface within the router to slow down.
input errors	Includes runts, giants, no buffer, CRC, frame, overrun, and ignored counts. Other input-related errors can also cause the input errors count to be increased, and some datagrams may have more than one error; therefore, this sum may not balance with the sum of enumerated input error counts.
CRC	Cyclic redundancy checksum generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a LAN, this is usually the result of collisions or a malfunctioning Ethernet device.
overrun	Number of times the receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver’s ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different from the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can increase the ignored count.
input packets with dribble condition detected	Dribble bit error indicates that a frame is slightly too long. This frame error counter is incremented just for informational purposes; the router accepts the frame.
packets output	Total number of messages transmitted by the system.
bytes	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the transmitter has been running faster than the router can handle. This may never be reported on some interfaces.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors, because some datagrams may have more than one error, and others may have errors that do not fall into any of the specifically tabulated categories.

Field	Description
collisions	Number of messages retransmitted because of an Ethernet collision. A packet that collides is counted only once in output packets.
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within several seconds. On a serial line, this can be caused by a malfunctioning modem that is not supplying the transmit clock signal, or by a cable problem. If the system notices that the carrier detect line of a serial interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an interface is looped back or shut down.
babbles **Note** This field applies to the router internal interface that connects to the installed Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT). This field typically does not apply to the external satellite interface.	Indicates that the transmit jabber timer expired.
late collision	Number of late collisions. Late collision happens when a collision occurs after the preamble has been transmitted. The most common cause of late collisions is that your Ethernet cable segments are too long for the speed at which you are transmitting.
deferred	Deferred indicates that the chip had to defer transmission while ready to transmit a frame, because the carrier was asserted.
lost carrier	Number of times the carrier was lost during transmission.
no carrier	Number of times the carrier was not present during the transmission.
output buffer failures	Number of failed buffers.
output buffers swapped out	Number of buffers swapped out.

Related Commands

Command	Description
service-module satellite status	Displays status information related to the hardware and software on the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT), including the initial configuration parameters.

Command	Description
show controllers satellite	Displays controller information about the internal router interface that connects to an installed Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT).

show interfaces serial

To display information about a serial interface, use the**showinterfacesserial** command in privileged EXEC mode. When using Frame Relay encapsulation, use the **showinterfacesserial** command in user EXEC or privileged EXEC mode to display information about the multicast data-link connection identifier (DLCI), the DLCIs used on the interface, and the DLCI used for the Local Management Interface (LMI).

Cisco 4000 Series
show interfaces serial accounting commandshow interfaces serial [*number* [**:** *channel-group*]] [**accounting**]

Cisco 7200 Series
show interfaces serial [*slot*/*port*] [**accounting**]

Cisco 7000 and Cisco 7500 Series with the RSP7000, RSP7000CI, or Ports on VIPs
show interfaces serial [*slot*/*port-adapter*/*port*]

Cisco 7500 Series
show interfaces serial [*slot*/*port* [**:** *channel-group*]] [**accounting**]

Cisco 7500 Series with a CT3IP
show interfaces serial [*slot*/*port-adapter*/*port*] [**:** *t1-channel*] [{**accounting** | **crb**}]

Cisco AS5350 and Cisco AS5400 Universal Gateways
show interfaces serial *slot*/*port*

Cisco AS5800 Access Servers
show interfaces serial *dial-shelf*/*slot*/*t3-port* **:** *t1-num* **:** *chan-group*

Syntax Description

number	(Optional) Number of the port being displayed.
: *channel-group*	(Optional) On the Cisco 4000 series with a Network Management Processor (NPM) or the Cisco 7500 series routers with a MultiChannel Interface Processor (MIP), specifies the T1 channel-group number in the range of 0 to 23 defined with the **channel-group** controller configuration command.
accounting	(Optional) Displays the number of packets of each protocol type that have been sent through the interface.
slot	(Optional) Number of the slot being displayed. Refer to the appropriate hardware manual for slot and port information.
/ *port*	(Optional) Number of the port being displayed. Refer to the appropriate hardware manual for slot and port information.
/ *port-adapter*	(Optional) Number of the port adapter being displayed. Refer to the appropriate hardware manual for information about port adapter compatibility.

: *t1-channel*	(Optional) T1 channel number. For the CT3IP, the T1 channel is a number between 1 and 28. T1 channels on the CT3IP are numbered 1 to 28 rather than the more traditional zero-based scheme (0 to 27) used with other Cisco products. This scheme ensures consistency with telco numbering schemes for T1 channels within channelized T3 equipment.
crb	(Optional) Displays interface routing and bridging information.
dial-shelf	Dial shelf chassis in the Cisco AS5800 access server that contains the CT3 interface card.
slot	Location of the CT3 interface card in the dial shelf chassis.
t3-port	T3 port number. The only valid value is 0.
: *t1-num*	T1 time slot in the T3 line. The value can be from 1 to 28.
: *chan-group*	Channel group identifier.

Command Modes

User EXEC (when Frame Relay encapsulation is used) Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced on the Cisco 4000 series routers.
11.0	This command was implemented on the Cisco 7000 series routers.
11.1CA	This command was modified to include sample output for the PA-2JT2, PA-E3, and PA-T3 serial port adapters.
11.3	This command was modified to include the CT3IP.
12.0(3)T	This command was implemented on the Cisco AS5800 access servers.
12.0(4)T	This command was modified to include enhanced display information for dialer bound interfaces.
12.2(11)T	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(13)T	This command was modified to display information about Frame Relay interface queueing and fragmentation.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Frame Relay

Use this command to determine the status of the Frame Relay link. This display also indicates Layer 2 status if switched virtual circuits (SVCs) are configured.

Channel Groups as Virtual Serial Interfaces

To find out about channel groups configured as virtual serial interfaces, to verify that the router has High-Level Data Link Control (HDLC) encapsulation on the interface, and to verify that the interface sees the loopback, use the **showinterfacesserial** command in privileged EXEC mode.

Examples

Example of Synchronous Serial Interface

The following is sample output from the **showinterfacesserial** command for a synchronous serial interface:

```
Router# show interfaces serial
Serial 0 is up, line protocol is up
   Hardware is MCI Serial
   Internet address is 192.168.10.203, subnet mask is 255.255.255.0
   MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
   Encapsulation HDLC, loopback not set, keepalive set (10 sec)
   Last input 0:00:07, output 0:00:00, output hang never
   Output queue 0/40, 0 drops; input queue 0/75, 0 drops
   Five minute input rate 0 bits/sec, 0 packets/sec
   Five minute output rate 0 bits/sec, 0 packets/sec
       16263 packets input, 1347238 bytes, 0 no buffer
       Received 13983 broadcasts, 0 runts, 0 giants
       2 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 2 abort
1 carrier transitions
     22146 packets output, 2383680 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets, 0 restarts
```

The table below describes significant fields shown in the display.

Table 144: show interfaces serial Field Descriptions--Synchronous Serial Interface

Field	Description
Serial ... is {up | down} ... is administratively down	Indicates whether the interface hardware is currently active (whether carrier detect is present), is currently inactive, or has been taken down by an administrator.
line protocol is {up | down}	Indicates whether the software processes that handle the line protocol consider the line usable (that is, whether keepalives are successful) or whether the line has been taken down by an administrator.
Hardware is	Specifies the hardware type.
Internet address is	Specifies the Internet address and subnet mask.
MTU	Maximum transmission unit of the interface.
BW	Indicates the value of the bandwidth parameter that has been configured for the interface (in kbps). If the interface is attached to a serial line with a line speed that does not match the default (1536 or 1544 kbps for T1 and 56 kbps for a standard synchronous serial line), use the **bandwidth**command to specify the correct line speed for this serial line.
DLY	Delay of the interface, in microseconds.

Field	Description
rely	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method assigned to interface.
loopback	Indicates whether or not loopback is set.
keepalive	Indicates whether or not keepalives are set.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This counter is updated only when packets are process-switched, not when packets are fast-switched.
Last output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by an interface. This counter is updated only when packets are process-switched, not when packets are fast-switched.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.
Output queue, drops input queue, drops	Number of packets in output and input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped because of a full queue.
5 minute input rate 5 minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes. The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernet networks and bursts of noise on serial lines are often responsible for no input buffer events.
Received... broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium.

Field	Description
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium.
input errors	Total number of no buffer, runts, giants, CRCs, frame, overrun, ignored, and abort counts. Other input-related errors can also increment the count, so that this sum might not balance with the other counts.
CRC	Cyclic redundancy checksum generated by the originating station or far-end device does not match the checksum calculated from the data received. On a serial link, CRCs usually indicate noise, gain hits, or other transmission problems on the data link.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a serial line, this is usually the result of noise or other transmission problems.
overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. Broadcast storms and bursts of noise can cause the ignored count to be increased.
abort	Illegal sequence of one bits on a serial interface. This usually indicates a clocking problem between the serial interface and the data link equipment.
carrier transitions	Number of times the carrier detect signal of a serial interface has changed state. For example, if data carrier detect (DCD) goes down and comes up, the carrier transition counter will increment two times. Indicates modem or line problems if the carrier detect line is changing state often.
packets output	Total number of messages transmitted by the system.
bytes output	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the transmitter has been running faster than the router can handle. This might never be reported on some interfaces.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface from being examined. Note that this might not balance with the sum of the enumerated output errors because some datagrams can have more than one error, and others can have errors that do not fall into any of the specifically tabulated categories.
collisions	Number of messages retransmitted because of an Ethernet collision. Some collisions are normal. However, if your collision rate climbs to around 4 or 5 percent, you should consider verifying that there is no faulty equipment on the segment and/or moving some existing stations to a new segment. A packet that collides is counted only once in output packets.

Field	Description
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within several seconds' time. On a serial line, this can be caused by a malfunctioning modem that is not supplying the transmit clock signal or by a cable problem. If the system notices that the carrier detect line of a serial interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an interface is looped back or shut down.
restarts	Number of times the controller was restarted because of errors.
alarm indications, remote alarms, rx LOF, rx LOS	Number of CSU/DSU alarms and number of occurrences of receive loss of frame and receive loss of signal.
BER inactive, NELR inactive, FELR inactive	Status of G.703-E1 counters for bit-error rate (BER) alarm, near-end loop remote (NELR), and far-end loop remote (FELR). Note that you cannot set the NELR or FELR.

Example of PA-2JT2 Serial Interface

The following is sample output from the **showinterfacesserial** command for a PA-2JT2 serial interface:

```
Router# show interfaces serial 3/0/0
Serial3/0/0 is up, line protocol is up
  Hardware is cyBus Serial
  Internet address is 10.0.0.1/8
  MTU 1500 bytes, BW 6312 Kbit, DLY 20000 usec, rely 255/255, load 26/255
  Encapsulation HDLC, loopback not set, keepalive not set
  Last input 00:04:31, output 00:04:31, output hang never
  Last clearing of "show interface" counters 00:06:07
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 162000 bits/sec, 8 packets/sec
  5 minute output rate 162000 bits/sec, 8 packets/sec
     20005 packets input, 20080520 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     20005 packets output, 20080520 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     0 cv errors, 0 crc5 errors, 0 frame errors
     rxLOS inactive, rxLOF inactive, rxPAIS inactive
     rxAIS inactive, rxRAI inactive, rxHBER inactive
```

The table below describes significant fields shown in the display that are different from the fields described in the table above.

Table 145: show interfaces serial Field Descriptions--PA-2JT2

Field	Description
Last clearing of “show interface” counters	Time the counters were last cleared.
Queueing strategy	First-in, first-out queueing strategy (other queueing strategies that you might see are priority-list, custom-list, and weighted fair).
output buffer failures	Number of “no resource” errors received on the output.
output buffers swapped out	Number of packets swapped to DRAM.
carrier transitions	Number of times the carrier detect signal of a serial interface has changed state. For example, if data carrier detect (DCD) goes down and comes up, the carrier transition counter will increment two times. Indicates modem or line problems if the carrier detect line is changing state often.
cv errors	B8ZS/B6ZS (zero suppression) coding violation counter.
crc5 errors	CRC-5 error counter.
frame errors	Framing error counter.
rxLOS	Receive loss of signal alarm. Values are active or inactive.
rxLOF	Receive loss of frame alarm. Values are active or inactive.
rxPAIS	Receive loss of payload alarm indication signal (AIS). Values are active or inactive.
rxAIS	Receive loss of physical AIS. Values are active or inactive.
rxRAI	Receive remote AIS. Values are active or inactive.
rxHBER	Receive high bit-error rate alarm. Values are active or inactive.

Example of PA-E3 Serial Port Adapter

The following is sample output from the **showinterfacesserial** command for a PA-E3 serial port adapter installed in chassis slot 2:

```
Router# show interfaces serial 2/0
Serial2/0 is up, line protocol is up
  Hardware is M1T-E3 pa
  Internet address is 172.17.1.1/24
  MTU 4470 bytes, BW 34010 Kbit, DLY 200 usec, rely 128/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive not set
  Last input 1w0d, output 00:00:48, output hang never
  Last clearing of “show interface” counters 1w0d
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
```

```
    20 packets input, 2080 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 parity
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    11472 packets output, 3824748 bytes, 0 underruns
    0 output errors, 0 applique, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions
  rxLOS inactive, rxLOF inactive, rxAIS inactive
  txAIS inactive, rxRAI inactive, txRAI inactive
```

Table 3 describes significant fields shown in the display that are different from the fields described in Table 1.

*Table 146: **show interfaces serial** Field Descriptions--PA-E3*

Field	Description
Last clearing of "show interface" counters	Time the counters were last cleared.
Queueing strategy	First-in, first-out queueing strategy (other queueing strategies that you might see are priority-list, custom-list, and weighted fair).
parity	Number of the parity errors on the interface.
applique	Indicates that an unrecoverable error has occurred on the E3 applique. The router then invokes an interface reset.
output buffer failures	Number of "no resource" errors received on the output.
output buffers swapped out	Number of packets swapped to DRAM.
rxLOS, rxLOF, rxAIS	Receive loss of signal, loss of frame, and alarm indication signal status. Values are inactive or active.
txAIS, rxRAI, txRAI	Transmit alarm indication signal, receive remote alarm indicator, and transmit remote alarm indicator status. Values are inactive or active. When the router receives an LOS, LOF, or AIS, the txRAI is active. When the remote router receives an LOS, LOF, or AIS, the rxRAI is active.

Example of 1-Port PA-T3 Serial Port Adapter Installed in a VIP2

The following is sample output from the **showinterfacesserial** command for a 1-port PA-T3 serial port adapter installed in a VIP2 in chassis slot 1, in port adapter slot 0:

```
Router# show interfaces serial 1/0/0
Serial1/0/0 is up, line protocol is up
  Hardware is cyBus PODS3 Serial
  Internet address is 172.18.1.1/24
  MTU 4470 bytes, BW 44736 Kbit, DLY 200 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input 00:00:05, output 00:00:02, output hang never
  Last clearing of "show interface" counters 5d02h
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 27269 drops
```

```
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     79039 packets input, 14195344 bytes, 0 no buffer
     Received 84506 broadcasts, 0 runts, 0 giants
              0 parity
     9574 input errors, 6714 CRC, 0 frame, 1 overrun, 0 ignored, 2859 abort
     62472 packets output, 13751644 bytes, 0 underruns
     0 output errors, 0 applique, 10 interface resets
     0 output buffer failures, 0 output buffers swapped out
     16 carrier transitions
   rxLOS inactive, rxLOF inactive, rxAIS inactive
   txAIS inactive, rxRAI inactive, txRAI inactive
```

The table below describes significant fields shown in the display that are different from the fields described in the tables above.

Table 147: show interfaces serial Field Descriptions--PA-T3

Field	Description
Last clearing of "show interface" counters	Time the counters were last cleared.
Queueing strategy	First-in, first-out queueing strategy (other queueing strategies that you might see are priority-list, custom-list, and weighted fair).
parity	Number of the parity errors on the interface.
applique	Indicates that an unrecoverable error has occurred on the T3 applique. The router then invokes an interface reset.
output buffer failures	Number of "no resource" errors received on the output.
output buffers swapped out	Number of packets swapped to DRAM.
rxLOS, rxLOF, rxAIS	Receive loss of signal, loss of frame, and alarm indication signal status. Values are inactive or active.
txAIS, rxRAI, txRAI	Transmit alarm indication signal, receive remote alarm indicator, and transmit remote alarm indicator status. Values are inactive or active. When the router receives an LOS, LOF, or AIS, the txRAI is active. When the remote router receives an LOS, LOF, or AIS, the rxRAI is active.

Example of CT3IP Serial Interface

The following is sample output from the **showinterfacesserial** command for the CT3IP serial interface:

```
Router# show interfaces serial 3/0/0:25
Serial3/0/0:25 is up, line protocol is up
  Hardware is cyBus T3
  Internet address is 10.25.25.2/24
  MTU 1500 bytes, BW 1536 Kbit, DLY 20000 usec, rely 255/255, load 12/255
  Encapsulation HDLC, loopback not set, keepalive not set
  Last input 00:19:01, output 00:11:49, output hang never
```

```
  Last clearing of "show interface" counters 00:19:39
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/64/0 (size/threshold/drops)
     Conversations 0/1 (active/max active)
     Reserved Conversations 0/0 (allocated/max allocated)
  5 minute input rate 69000 bits/sec, 90 packets/sec
  5 minute output rate 71000 bits/sec, 90 packets/sec
     762350 packets input, 79284400 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants
     150 input errors, 0 CRC, 0 frame, 150 overrun, 0 ignored, 0 abort
     763213 packets output, 80900472 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions no alarm present
  Timeslot(s) Used:1-24, Transmitter delay is 0 flags, transmit queue length 5
  non-inverted data
```

The table below describes significant fields relevant to the CT3IP shown in the display that are different from the fields described in the tables above.

*Table 148: **show interfaces serial** Field Descriptions--CT3IP*

Field	Description
Timeslot(s) Used	Number of time slots assigned to the T1 channel.
Transmitter delay	Number of idle flags inserted between each HDLC frame.
transmit queue length	Number of packets allowed in the transmit queue.
non-inverted data	Indicates whether or not the interface is configured for inverted data.

Example of an HDLC Synchronous Serial Interface on a Cisco 7500 Series Router

The following is sample output from the **showinterfacesserial** command for an HDLC synchronous serial interface on a Cisco 7500 series router:

```
Router# show interfaces serial 1/0
Serial1/0 is up, line protocol is up
  Hardware is cxBus Serial
  Internet address is 172.19.190.203, subnet mask is 255.255.255.0
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input 0:00:07, output 0:00:00, output hang never
  Last clearing of "show interface" counters 2w4d
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  Five minute input rate 0 bits/sec, 0 packets/sec
  Five minute output rate 0 bits/sec, 0 packets/sec
     16263 packets input, 1347238 bytes, 0 no buffer
     Received 13983 broadcasts, 0 runts, 0 giants
     2 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 2 abort
     22146 packets output, 2383680 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets, 0 restarts
     1 carrier transitions
```

The tables above describes significant fields shown in the display.

Example of HDLC Encapsulation

The following example displays High-Level Data Link Control (HDLC) encapsulation on serial interface 0:

```
Router# show interfaces serial 0
Serial0 is up, line protocol is up (looped)
Hardware is HD64570
Internet address is 10.1.1.1, subnet mask is 255.255.255.0
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation HDLC, loopback set, keepalive set (10 sec)
```

The tables above describes significant fields shown in the display.

Example of a G.703 Interface with Framing

The following is sample output from the **showinterfacesserial** command for a G.703 interface on which framing is enabled:

```
Router# show interfaces serial 2/3
Serial2/3 is up, line protocol is up
  Hardware is cxBus Serial
  Internet address is 10.4.4.1, subnet mask is 255.255.255.0
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive not set
  Last input 0:00:21, output 0:00:21, output hang never
  Last clearing of "show interface" counters never
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  Five minute input rate 0 bits/sec, 0 packets/sec
  Five minute output rate 0 bits/sec, 0 packets/sec
     53 packets input, 7810 bytes, 0 no buffer
     Received 53 broadcasts, 0 runts, 0 giants
     2 input errors, 2 CRC, 0 frame, 0 overrun, 0 ignored, 2 abort
     56 packets output, 8218 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets, 0 restarts
     1 carrier transitions
     2 alarm indications, 333 remote alarms, 332 rx LOF, 0 rx LOS
     RTS up, CTS up, DTR up, DCD up, DSR up
     BER inactive, NELR inactive, FELR inactive
```

The tables above describes significant fields shown in the display.

Example with Frame Relay Encapsulation

When using Frame Relay encapsulation, use the **showinterfacesserial**command to display information on the multicast data-link connection identifier (DLCI), the DLCI of the interface, and the DLCI used for the local management interface (LMI).

The multicast DLCI and the local DLCI can be set using the **frame-relaymulticast-dlci** and **frame-relaylocal-dlci** configuration commands. The status information is taken from the LMI, when active.

The following is sample output from the **showinterfacesserial** command when Frame Relay encapsulation and LMI are enabled:

```
Router# show interfaces serial
Serial 2 is up, line protocol is up
   Hardware type is MCI Serial
   Internet address is 172.20.122.1, subnet mask is 255.255.255.0
   MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
   Encapsulation FRAME-RELAY, loopback not set, keepalive set (10 sec)
   multicast DLCI 1022, status defined, active
   source DLCI    20, status defined, active
   LMI DLCI 1023, LMI sent 10, LMI stat recvd 10, LMI upd recvd 2
   Last input 7:21:29, output 0:00:37, output hang never
   Output queue 0/100, 0 drops; input queue 0/75, 0 drops
   Five minute input rate 0 bits/sec, 0 packets/sec
   Five minute output rate 0 bits/sec, 0 packets/sec
       47 packets input, 2656 bytes, 0 no buffer
       Received 5 broadcasts, 0 runts, 0 giants
       5 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 57 abort
       518 packets output, 391205 bytes
       0 output errors, 0 collisions, 0 interface resets, 0 restarts
       1 carrier transitions
```

In this display, the multicast DLCI has been changed to 1022 using the **frame-relaymulticast-dlci** interface configuration command.

The display shows the statistics for the LMI as the number of status inquiry messages sent (LMI sent), the number of status messages received (LMI recvd), and the number of status updates received (upd recvd). Refer to the Frame Relay Interface specification for additional explanations of this output.

Example with Frame Relay Queueing and Fragmentation at the Interface

The default mode for Frame Relay interfaces on serial SPAs is transparent mode. When FRF.12 configuration is applied to these SPA interfaces, then the SPA interface mode changes to end-to-end.

With end-to-end configuration on CEs, L2VPN cloud on GSR PEs can transparently forward the FRF.12 fragments to remote CE by default. In case of L2VPN on Cisco 12000 series Internet router, FRF.12 configuration should not be applied on the main or sub-interfaces of SPA interfaces. Otherwise the FRF.12 fragments get dropped in ingress interface on SPA on the ingress PE.

For L3VPN to work on Cisco 12000 series Internet router, FRF.12 configuration needs to be applied to the L3VPN SPA interface (main or sub-interface). L3VPN will not work without FRF.12 configuration.

L2VPN requires the SPA interface to be in transparent mode. L3VPN requires the SPA interface to be in end-to-end mode. At physical interface level, either L2VPN or L3VPN works at a time. Both L2VPN and L3VPN will not work simultaneously on a single physical interface. FRF.12 configuration applied on a L3VPN sub-interface, changes the mode of the entire physical interface to end-to-end and all L2VPN sub-interface traffic on this physical interface gets dropped.

If L2VPN circuits are already present on a SPA interface and FRF.12 configuration is applied on this interface, then the following error message will be displayed to indicate FRF.12 fragment drops on L2VPN circuits.

SLOT 3:2d08h: %GLCFR-3-FR_MODE: (bflc_fr_xdr_cmd_vc_status)FRF12 fragments will be dropp

The following is sample output from the **showinterfacesserial** command when low-latency queueing and FRF.12 end-to-end fragmentation are configured on a Frame Relay interface:

```
Router# show interfaces serial 3/2
Serial3/2 is up, line protocol is up
  Hardware is M4T
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY, crc 16, loopback not set
  Keepalive set (10 sec)
  LMI enq sent  0, LMI stat recvd 0, LMI upd recvd 0, DTE LMI up
  LMI enq recvd 0, LMI stat sent  0, LMI upd sent  0
  LMI DLCI 1023  LMI type is CISCO  frame relay DTE
  Fragmentation type: end-to-end, size 80, PQ interleaves 0
  Broadcast queue 0/64, broadcasts sent/dropped 0/0, interface broadcasts 0
  Last input 2d15h, output 2d15h, output hang never
  Last clearing of "show interface" counters 00:01:31
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1094 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 output buffer failures, 0 output buffers swapped out
     1 carrier transitions     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

The table below describes significant fields shown in the display that are different from the fields described in the tables above.

*Table 149: **show interfaces serial** Field Descriptions--Frame Relay Interface Queueing and Fragmentation*

Field	Description
txload	Interface load in the transmit direction.
rxload	Interface load in the receive direction.
crc	Length the cyclic redundancy check (CRC) used on the interface.
LMI enq sent	Number of Frame Relay status inquiry messages sent.
LMI stat recvd	Number of Frame Relay status request messages received.
LMI upd recvd	Number of single PVC asynchronous status messages received.
DTE LMI up	LMI peers are synchronized.
LMI enq recvd	Number of Frame Relay status inquiry messages received.
LMI stat sent	Number of Frame Relay status request messages sent.
LMI upd sent	Number of single PVC asynchronous status messages sent.
Fragmentation type	Type of fragmentation: end-to-end, Cisco, or VoFR

Field	Description
size	Fragmentation size.
PQ interleaves	Number of priority queue frames that have interleaved data fragments.
Broadcast queue	Number on queue/queue depth.
broadcasts sent/dropped	Number of broadcasts sent and dropped.
interface broadcasts	Number of broadcasts sent on interface.
Input queue	size--Current size of the input queue. max--Maximum size of the queue. drops--Number of messages discarded. flushes--Number of times that data on queue has been discarded.
Queueing strategy	Type of queueing configured on the interface.
Output queue	size--Current size of the output queue. max total--Maximum number of frames that can be queued. threshold--Congestive-discard threshold. Number of messages in the queue after which new messages for high-bandwidth conversations are dropped. drops--Number of dropped messages.
Conversations	active--Number of currently active conversations. max active--Maximum number of conversations that have ever occurred at one time. max total--Maximum number of active conversations allowed.
throttles	Number of times the receiver on the port was disabled, possibly because of processor or buffer overload.
output buffer failures	Number of “no resource” errors received on the output.
output buffers swapped out	Number of packets swapped to DRAM.

Example with ANSI LMI

For a serial interface with the ANSI Local Management Interface (LMI) enabled, use the **showinterfacesserial**command to determine the LMI type implemented. The following is sample output from the **showinterfacesserial**command for a serial interface with the ANSI LMI enabled:

```
Router# show interfaces serial
Serial 1 is up, line protocol is up
   Hardware is MCI Serial
   Internet address is 172.18.121.1, subnet mask is 255.255.255.0
   MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
   Encapsulation FRAME-RELAY, loopback not set, keepalive set
   LMI DLCI    0, LMI sent 10, LMI stat recvd 10
   LMI type is ANSI Annex D
   Last input 0:00:00, output 0:00:00, output hang never
   Output queue 0/40, 0 drops; input queue 0/75, 0 drops


   Five minute input rate 0 bits/sec, 1 packets/sec
   Five minute output rate 1000 bits/sec, 1 packets/sec
       261 packets input, 13212 bytes, 0 no buffer
```

```
Received 33 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
238 packets output, 14751 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets, 0 restarts
```

Notice that the **showinterfacesserial**output for a serial interface with ANSI LMI shown in this display is very similar to that for encapsulation set to Frame Relay, as shown in the previous display. The table below describes the few differences that exist.

Table 150: show interfaces serial Field Descriptions--ANSI LMI

Field	Description
LMI DLCI 0	Identifies the DLCI used by the LMI for this interface. The default is 1023.
LMI sent 10	Number of LMI packets that the router sent.
LMI type is ANSI Annex D	Indicates that the interface is configured for the ANSI-adopted Frame Relay specification T1.617 Annex D.

Example with LAPB Encapsulation

Use the **showinterfacesserial**command to display operation statistics for an interface that uses Link Access Procedure, Balanced (LAPB) encapsulation. The following is partial sample output from the **showinterfacesserial** command for a serial interface that uses LAPB encapsulation:

```
Router# show interfaces serial 1
LAPB state is SABMSENT, T1 3000, N1 12056, N2 20, k7,Protocol ip
VS 0, VR 0, RCNT 0, Remote VR 0, Retransmissions 2
IFRAMEs 0/0 RNRs 0/0 REJs 0/0 SABMs 3/0 FRMRs 0/0 DISCs 0/0
```

The table below shows the fields relevant to all LAPB connections.

Table 151: show interfaces serial Field Descriptions--LAPB

Field	Description
LAPB state is	State of the LAPB protocol.
T1 3000, N1 12056, ...	Current parameter settings.
Protocol	Protocol encapsulated on a LAPB link; this field is not present on interfaces configured for multiprotocol LAPB or X.25 encapsulations.
VS	Modulo 8 frame number of the next outgoing information frame.
VR	Modulo 8 frame number of the next information frame expected to be received.
RCNT	Number of received information frames that have not yet been acknowledged.
Remote VR	Number of the next information frame that the remote device expects to receive.
Retransmissions	Count of current retransmissions because of expiration of T1.

Field	Description
Window is closed	No more frames can be transmitted until some outstanding frames have been acknowledged. This message should be displayed only temporarily.
IFRAMEs	Count of information frames in the form of sent/received.
RNRs	Count of Receiver Not Ready frames in the form of sent/received.
REJs	Count of Reject frames in the form of sent/received.
SABMs	Count of Set Asynchronous Balanced Mode commands in the form of sent/received.
FRMRs	Count of Frame Reject frames in the form of sent/received.
DISCs	Count of Disconnect commands in the form of sent/received.

Example with PPP Encapsulation

The output for an interface configured for synchronous PPP encapsulation differs from the standard **showinterfacesserial** output. An interface configured for PPP might include the following information:

```
Router# show interfaces serial 1
lcp state = OPEN
ncp ipcp state = OPEN   ncp osicp state = NOT NEGOTIATED
ncp ipxcp state = NOT NEGOTIATED   ncp deccp state = NOT NEGOTIATED
ncp bridgecp state = NOT NEGOTIATED   ncp atalkcp state = NOT NEGOTIATED
```

The table below show the fields relevant to PPP connections.

Table 152: show interfaces serial Field Descriptions--PPP Encapsulation

Field	Description
lcp state	Link Control Protocol.
ncp ipcp state	Network Control Protocol Internet Protocol Control Protocol.
ncp osicp state	Network Control Protocol OSI (CLNS) Control Protocol.
ncp ipxcp state	Network Control Protocol IPX (Novell) Control Protocol.
ncp deccp state	Network Control Protocol DECnet Control Protocol.
ncp bridgecp state	Network Control Protocol Bridging Control Protocol.
ncp atalkcp state	Network Control Protocol AppleTalk Control Protocol.

Example with SDLC Connections

Use the **showinterfacesserial**command to display the Synchronous Data Link Control (SDLC) information for a given SDLC interface. The following is sample output from the **showinterfacesserial**command for an SDLC primary interface that supports the SDLLC function:

```
Router# show interfaces serial
Serial 0 is up, line protocol is up
Hardware is MCI Serial
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation SDLC-PRIMARY, loopback not set
    Timers (msec): poll pause 100 fair poll 500. Poll limit 1
    [T1 3000, N1 12016, N2 20, K 7] timer: 56608 Last polled device: none
    SDLLC [ma: 0000.0C01.14--, ring: 7 bridge: 1, target ring: 10
             largest token ring frame 2052]
SDLC addr C1 state is CONNECT
     VS 6, VR 3, RCNT 0, Remote VR 6, Current retransmit count 0
     Hold queue: 0/12 IFRAMEs 77/22 RNRs 0/0 SNRMs 1/0 DISCs 0/0
     Poll: clear, Poll count: 0, chain: p: C1 n: C1
     SDLLC [largest SDLC frame: 265, XID: disabled]
 Last input 00:00:02, output 00:00:01, output hang never
 Output queue 0/40, 0 drops; input queue 0/75, 0 drops
 Five minute input rate 517 bits/sec, 30 packets/sec
 Five minute output rate 672 bits/sec, 20 packets/sec
     357 packets input, 28382 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     926 packets output, 77274 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets, 0 restarts
     2 carrier transitions
```

The table below shows the fields relevant to all SDLC connections.

Table 153: show interfaces serial Field Descriptions--SDLC Enabled

Field	Description
Timers (msec): poll pause, fair poll, Poll limit	Current values of these timers for the primary SDLC interface.
T1, N1, N2, K	Values for these parameters for the primary SDLC interface.

The table below shows other data given for each SDLC secondary interface configured to be attached to the serial interface.

Table 154: SDLC Secondary Interface Descriptions

Field	Description
addr	Address of this SDLC secondary interface.

Field	Description
state is	Current state of this connection, which is one of the following: • DISCONNECT--No communication is being attempted to this secondary. • CONNECT--A normal connect state exists between this router and this secondary. • DISCSENT--This router has sent a disconnect request to this secondary and is awaiting its response. • SNRMSENT--This router has sent a connect request (SNRM) to this secondary and is awaiting its response. • THEMBUSY--This secondary has told this router that it is temporarily unable to receive any more information frames. • USBUSY--This router has told this secondary that it is temporarily unable to receive any more information frames. • BOTHBUSY--Both sides have told each other that they are temporarily unable to receive any more information frames. • ERROR--This router has detected an error and is waiting for a response from the secondary acknowledging this.
VS	Sequence number of the next information frame that this station sends.
VR	Sequence number of the next information frame from this secondary that this station expects to receive.
Remote VR	Last frame transmitted by this station that has been acknowledged by the other station.
Current retransmit count:	Number of times the current I-frame or sequence of I-frames has been retransmitted.
Hold Queue	Number of frames in hold queue and maximum size of hold queue.
IFRAMEs, RNRs, SNRMs, DISCs	Sent/received count for these frames.
Poll	“Set” if this router has a poll outstanding to the secondary; “clear” if it does not.
Poll Count	Number of polls in a row that have been given to this secondary at this time.
Chain	Shows the previous (p) and next (n) secondary address on this interface in the *roundrobinloop* of polled devices.

Example with SDLLC

Use the **showinterfacesserial**command to display the SDLLC statistics for SDLLC-configured interfaces. The following is sample output from the **showinterfacesserial**command for a serial interface configured for SDLLC:

```
Router# show interfaces serial
Serial 0 is up, line protocol is up
   Hardware is MCI Serial
   MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
   Encapsulation SDLC-PRIMARY, loopback not set
       Timers (msec): poll pause 100 fair poll 500. Poll limit 1
       [T1 3000, N1 12016, N2 20, K 7] timer: 56608 Last polled device: none
       SDLLC [ma: 0000.0C01.14--, ring: 7 bridge: 1, target ring: 10
             largest token ring frame 2052]
   SDLC addr C1 state is CONNECT
       VS 6, VR 3, RCNT 0, Remote VR 6, Current retransmit count 0
       Hold queue: 0/12 IFRAMEs 77/22 RNRs 0/0 SNRMs 1/0 DISCs 0/0
       Poll: clear, Poll count: 0, chain: p: C1 n: C1
       SDLLC [largest SDLC frame: 265, XID: disabled]
   Last input 00:00:02, output 00:00:01, output hang never
   Output queue 0/40, 0 drops; input queue 0/75, 0 drops
   Five minute input rate 517 bits/sec, 30 packets/sec
   Five minute output rate 672 bits/sec, 20 packets/sec
       357 packets input, 28382 bytes, 0 no buffer
       Received 0 broadcasts, 0 runts, 0 giants
       0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
       926 packets output, 77274 bytes, 0 underruns
       0 output errors, 0 collisions, 0 interface resets, 0 restarts
       6608 Last polled device: none
       SDLLC [ma: 0000.0C01.14--, ring: 7 brid2 carrier transitions
```

Most of the output shown in the display is generic to all SDLC-encapsulated interfaces and is described in the *CiscoIOS Bridging and IBM Networking Command Reference* , *Volume 2 of 2: IBM Networking* . The table below shows the parameters specific to SDLLC.

Table 155: SDLLC Parameter Descriptions

Field	Description
SDLLC ma	Lists the MAC address configured for this interface. The last byte is shown as "--" to indicate that it is filled in with the SDLC address of the connection.
ring, bridge, target ring	Lists the parameters as configured by the **sdllctraddr**command.
largest token ring frame	Shows the largest Token Ring frame that is accepted on the Logical Link control, type 2 (LLC2) side of the connection.
largest SDLC frame	Shows the largest SDLC frame that is accepted and will be generated on the SDLC side of the connection.
XID	Enabled or disabled: Shows whether XID processing is enabled on the SDLC side of the connection. If enabled, it will show the XID value for this address.

Example with X.25

The following is partial sample output from the **showinterfacesserial**command for a serial X.25 interface:

```
Router# show interfaces serial 1
X25 address 000000010100, state R1, modulo 8, idle 0, timer 0, nvc 1
  Window size: input 2, output 2, Packet size: input 128, output 128
  Timers: T20 180, T21 200, T22 180, T23 180, TH 0
  Channels: Incoming-only none, Two-way 1-1024, Outgoing-only none
(configuration on RESTART: modulo 8,
  Window size: input 2 output 2, Packet size: input 128, output 128
  Channels: Incoming-only none, Two-way 5-1024, Outgoing-only none)
  RESTARTs 3/2 CALLs 1000+2/1294+190/0+0/ DIAGs 0/0
```

The stability of the X.25 protocol requires that some parameters not be changed without a restart of the protocol. Any change to these parameters is held until a restart is sent or received. If any of these parameters changes, information about the router configuration at restart will be displayed as well as the values that are currently in effect.

The table below describes significant fields shown in the display.

Table 156: show interfaces serial Field Descriptions--X.25 Enabled

Field	Description
X25 address	Address used to originate and accept calls.
state	State of the interface. Possible values follow: • R1 is the normal ready state. • R2 is the DTE restarting state. • R3 is the DCE restarting state. If the state is R2 or R3, the interface is awaiting acknowledgment of a Restart packet.
modulo	Modulo value; determines the packet sequence numbering scheme used.
idle	Number of minutes for which the Cisco IOS software waits before closing idle virtual circuits that it originated or accepted.
timer	Value of the interface timer, which is zero unless the interface state is R2 or R3.
nvc	Default maximum number of simultaneous virtual circuits permitted to and from a single host for a particular protocol.
Window size: input, output	Default window sizes (in packets) for the interface. The **x25facility** interface configuration command can be used to override these default values for the switched virtual circuits originated by the router.
Packet size: input, output	Default maximum packet sizes (in bytes) for the interface. The **x25facility** interface configuration command can be used to override these default values for the switched virtual circuits originated by the router.

Field	Description
Timers:	Values of the X.25 timers: • T10 through T13 for a DCE device • T20 through T23 for a DTE device
TH	Packet acknowledgment threshold (in packets). This value determines how many packets are received before an explicit acknowledgment is sent. The default value (0) sends an explicit acknowledgment only when the incoming window is full.
Channels: Incoming-only, Two-way, Outgoing-only	Displays the virtual circuit ranges for this interface.
RESTARTs	Shows Restart packet statistics for the interface using the format Sent/Received.
CALLs	Successful calls sent + failed calls/calls received + calls failed/calls forwarded + calls failed. Calls forwarded are counted as calls sent.
DIAGs	Diagnostic messages sent and received.

Example with Accounting Option

The following example illustrates the **showinterfacesserial** command with the **accounting** option on a Cisco 7500 series routers:

```
Router# show interfaces serial 1/0 accounting
Serial1/0
       Protocol    Pkts In   Chars In   Pkts Out  Chars Out
             IP       7344    4787842       1803    1535774
      Appletalk      33345    4797459      12781    1089695
        DEC MOP          0          0        127       9779
            ARP          7        420         39       2340
```

The table below describes thefields shown in the display.

*Table 157: **show interfaces serial** Field Descriptions--Accounting*

Field	Description
Protocol	Protocol that is operating on the interface.
Pkts In	Number of packets received for that protocol.
Chars In	Number of characters received for that protocol.
Pkts Out	Number of packets transmitted for that protocol.
Chars Out	Number of characters transmitted for that protocol.

Example with Cisco AS5800 Access Server

The following example shows the activity that occurred on the serial interface in shelf 1, slot 4, port 0 for time slot 2 in group 23:

```
Router# show interfaces serial 1/4/0:2:23
Serial1/4/0:2:23 is up, line protocol is up (spoofing)
 Hardware is DS-T1
 MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
 Encapsulation HDLC, loopback not set
 Last input 00:00:01, output 00:00:01, output hang never
 Last clearing of "show interface" counters 22:24:30
 Queueing strategy: fifo
 Output queue 0/40, 0 drops; input queue 0/75, 0 drops
 5 minute input rate 0 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
     5274 packets input, 20122 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     5274 packets output, 30836 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     2 carrier transitions no alarm present
 Timeslot(s) Used:24, subrate: 64Kb/s, transmit delay is 0 flags
```

The table below describes the significant fields shown in thedisplay that are different from the fields described in the tables above.

Table 158: show interfaces serial Command Field Descriptions--Cisco AS5800

Field	Description
Last clearing of “show interface” counters	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) were last reset to zero.
Queueing strategy	Displays the type of queueing configured for this interface. In the example output, the type of queueing configured is FIFO.
throttles	Number of times that the receiver on the port was disabled, possibly because of buffer or processor overload.
output buffer failures	Number of times that the output buffer has failed.
output buffer swapped out	Number of times that the output buffer has been swapped out.
Timeslot(s) Used	Number of time slots assigned to the T1 channel.
subrate	Bandwidth of each time slot.
transmit delay is ...	Number of idle flags inserted between each frame.

Related Commands

Command	Description
show controllers serial	Displays information about the virtual serial interface.

show interfaces sm

To display status, traffic data, and configuration information about the SM-SRE service module interface, use the **showinterfacessm** command in user EXEC or privileged EXEC mode.

show interfaces sm *slot*/*port*

Syntax Description

slot	Router slot in which the service module is installed. Range: 1 to 4.
/ *port*	Port number of the module interface. The slash mark (/) is required.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

The service module interface is the Gigabit Ethernet interface on the router that connects to the SM-SRE.

Examples

The following example displays status, traffic data, and configuration information about the interface to the SM-SRE installed in the router.

```
Router# show interfaces sm 1/0
SM1/0 is up, line protocol is up
  Hardware is PSE2, address is 001e.4a97.644d (bia 001e.4a97.644d)
  Internet address is 30.0.0.1/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s, media type is internal
  output flow-control is XON, input flow-control is XON
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:13, output 00:00:04, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/60 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     22 packets input, 1398 bytes, 0 no buffer
     Received 3 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     134 packets output, 42720 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

The table below describes the significant fields shown in the display.

Table 159: show interfaces sm Field Descriptions

Field	Description
Hardware, address	Hardware type and address.
MTU	Maximum transmission unit (MTU) of the service module interface.
BW	Bandwidth of the interface, in kbps.
DLY	Delay of the interface, in microseconds.
reliability	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
txload	Transmit load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
rxload	Receive load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method assigned to the interface.
loopback	Indicates whether or not loopback is set.
Keepalive	Indicates whether or not keepalives are set and the interval between keepalives if they have been set.
ARP type...ARP Timeout	Type of Address Resolution Protocol (ARP) assigned and length of timeout.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by the interface and processed locally on the router. This field is useful for detecting when a dead interface failed. **Note** This field is not updated by fast-switched traffic.
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by the interface. This field is useful for detecting when a dead interface failed.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because a transmission took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. Asterisks (***) indicate that the elapsed time is too large to be displayed.

Field	Description
Input queue	Number of packets in the input queue. Each number is followed by a slash, the maximum size of the queue, the number of packets dropped because of a full queue, and the number of times that queued packets have been discarded.
Total output drops	Number of packets in the output queue that have been dropped because of a full queue.
Queueing strategy	Queueing strategy applied to the interface, which is configurable under the interface. The default is FIFO (first-in, first-out).
Output queue	Number of packets in the output queue, and the maximum size of the queue. Each number is followed by a slash.
5 minute input rate, 5 minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic that it sends and receives (rather than all network traffic). The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within 2 percent of the instantaneous rate of a uniform stream of traffic over that period. **Note** The 5-minute period referenced in this output is a load interval that is configurable under the interface. The default value is 5 minutes.
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernets and bursts of noise on serial lines are often responsible for no input buffer events.
Received...broadcasts	Number of broadcasts received.
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium. For instance, any Ethernet packet that is less than 64 bytes is considered a runt.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium. For example, any Ethernet packet that is greater than 1518 bytes is considered a giant.
throttles	Number of times that the interface requested another interface within the router to slow down.

Field	Description
input errors	Errors that include runts, giants, no buffer, cyclic redundancy checksum (CRC), frame, overrun, and ignored counts. Other input-related errors can also cause the input errors count to be increased, and some datagrams may have more than one error; therefore, this sum may not balance with the sum of enumerated input error counts.
CRC	Errors created when the CRC generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station that is transmitting bad data.
frame	Number of packets received incorrectly that have a CRC error and a noninteger number of octets. On a LAN, this is usually the result of collisions or a malfunctioning Ethernet device.
overrun	Number of times that the receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets that were ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different from system buffer space described. Broadcast storms and bursts of noise can cause the ignored count to increase.
input packets with dribble condition detected	Number of packets with dribble condition. Dribble bit error indicates that a frame is slightly too long. This frame error counter is incremented just for informational purposes; the router accepts the frame.
packets output	Total number of messages that have been transmitted by the system.
bytes	Total number of bytes, including data and MAC encapsulation, that have been transmitted by the system.
underruns	Number of times that the transmitter has run faster than the router could handle. This may never be reported on some interfaces.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface that is being examined. Note that this may not balance with the sum of the enumerated output errors, because some datagrams may have more than one error, and others may have errors that do not fall into any of the specifically tabulated categories.
collisions	Number of messages that have been retransmitted because of an Ethernet collision. This is usually the result of an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). A packet that collides is counted only once in output packets.

Field	Description
interface resets	Number of times an interface has been completely reset. This can happen if packets that were queued for transmission were not sent within several seconds. On a serial line, this can be caused by a malfunctioning modem that is not supplying the transmit clock signal or by a cable problem. If the system notices that the carrier detect line of a serial interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an interface is looped back or shut down.
babbles	Count of frames greater than 1518 bytes that have been transmitted, indicating that the transmitter has been on the interface longer than the time necessary to transmit the largest frame.
late collision	Number of late collisions. A collision becomes a late collision when it occurs after the preamble has been transmitted.
deferred	Deferred indicates that the chip, while ready to transmit a frame, had to defer because the carrier was asserted.
lost carrier	Number of times that the carrier was lost during transmission.
no carrier	Number of times that the carrier was not present during the transmission.
output buffer failures, output buffers swapped out	Number of failed buffers and number of buffers swapped out.

Related Commands

Command	Description
show controllers sm	Displays controller information for the service module interface.

show interfaces status

To display the interface status or a list of interfaces in an error-disabled state on local area network (LAN) ports only, use the **showinterfacesstatus** command in user EXEC or privileged EXEC mode.

show interfaces [*interface interface-number*] **status** [{**err-disabled** | **module** *number* | **vlan** *vlan*}]

Syntax Description

interface	(Optional) Interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **pos**, **atm**, and **ge-wan**.
interface-number	(Optional) Module and port number; see the "Usage Guidelines" section for valid values.
err-disabled	(Optional) Displays the LAN ports in an error-disabled state.
module *number*	(Optional) Specifies the module number; see the "Usage Guidelines" section for valid values.
vlan *vlan*	(Optional) Specifies a VLAN. Limits the display of switch port information to the specified VLAN. Range: 1 to 4094.

Command Default

This command has no default settings.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17b)SXA	This command was changed to include the packet-buffer error status in the **showinterfacesstatuserr-disabled** output.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB. This command was changed to include the type string of the receive-only transceivers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXI	This command was changed to add the optional **vlan***vlan* keyword and argument.

Usage Guidelines

The *interface-number*argument designates the module and port number. Valid values for *interface-number* depend on the chassis and module that are used. For example, if you have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the slot number are from 1 to 13 and valid values for the port number are from 1 to 48.

This command is supported on LAN ports only.

The **module***number* keyword and argument designate the module number and limit the display to the interfaces on the module. Valid values depend on the chassis that is used. For example, if you have a 13-slot chassis, valid values for the module number are from 1 to 13.

To find out if an interface is inactive, enter the **showinterfacesstatus** command. If the interface is inactive, the Status field displays "inactive." If the port is not inactive, the Status field displays "none."

To find the packet and byte count, you can enter the **showinterfacescounters** command or the show **interfaces***interfaceinterface-number* status command. The **showinterfacescounters** command is the preferred command to use. In some cases, the packet and byte count of the show **interfaces***interfaceinterface-number* status command is incorrect.

Examples

This example shows how to display the status of all LAN ports:

```
Router>
show interfaces status
Port    Name               Status     Vlan       Duplex Speed Type
Gi1/1                      disabled   routed       full  1000 missing
Gi1/2                      notconnect 1            full  1000 unknown (4)
Fa5/1                      disabled   routed       auto  auto 10/100BaseTX
.
.
.
Port    Name               Status       Vlan       Duplex  Speed Type
Fa5/18                     disabled     1          auto    auto  10/100BaseTX
Fa5/19                     disabled     1          auto    auto  10/100BaseTX
Gi7/1                      disabled     1          full    1000  WDM-RXONLY
Gi7/2                      disabled     1          full    1000  No Transceiver
Router>
```

This example shows how to display the packet and byte count of a specific LAN port:

```
Router
> show interfaces fastethernet 5/2 status
FastEthernet5/2
Switching path    Pkts In   Chars In   Pkts Out  Chars Out
               Processor         17       1220         20       2020
             Route cache          0          0          0          0
       Distributed cache         17       1220  206712817 2411846570
                   Total         34       2440  206712837 2411848590
Router>
```

This example shows how to display the status of LAN ports in an error-disabled state:

```
Router>

show interfaces status
 err-disabled
Port    Name               Status       Reason
Fa9/4                      notconnect   link-flap
informational error message when the timer expires on a cause
--------------------------------------------------------------
5d04h:%PM-SP-4-ERR_RECOVER:Attempting to recover from link-flap err-disable state on Fa9/4
Router>
```

Catalyst 6500 Series Switches

The following shows how to display the **showinterfacesstatus**for VLAN 2:

```
Router# show interfaces status vlan 2
```

Related Commands

Command	Description
errdisable detect cause	Enables the error-disable detection.
show errdisable recovery	Displays the information about the error-disable recovery timer.

show interfaces summary

To display a summary of statistics for one interface or for all interfaces that are configured on a networking device, use the **show interfaces summary** command in privileged EXEC mode. For Cisco 7600 series routers, the command can also be used in user EXEC mode.

show interfaces summary

Cisco 7600 Series
show interfaces [*type number*] **summary** [**vlan**]

Syntax Description

type	(Optional) Interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **pos**, **atm**, and **ge-wan**.
number	(Optional) Module and port number of the specified interface.
vlan	(Optional) Displays the total number of VLAN interfaces .

Command Default

This command has no default settings.

Command Modes

Privileged EXEC. User EXEC (Cisco 7600 series only)

Command History

Release	Modification
12.2	This command was introduced.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S.

Usage Guidelines

Cisco 7600 Series

On a Cisco 7600 series router, you can display summary information for a single interface by specifying the interface type and number. Separate counters for subinterfaces are not maintained and are not displayed in the output.

Examples

The following is sample output from the **show interfaces summary** command:

```
Router# show interfaces summary
 *: interface is up
 IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
 RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
 TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
 TRTL: throttle count
  Interface          IHQ   IQD  OHQ   OQD  RXBS RXPS  TXBS TXPS  TRTL
```

```
----------------------------------------------------------------------
* FastEthernet0/0       0     0    0     0     0    0     0    0   0
  Serial0/0             0     0    0     0     0    0     0    0   0
  FastEthernet0/1       0     0    0     0     0    0     0    0   0
  Serial0/1             0     0    0     0     0    0     0    0   0
NOTE:No separate counters are maintained for subinterfaces
     Hence Details of subinterface are not shown.
```

This example shows how to display the total number of VLAN interfaces on a Cisco 7600 series router:

```
Router# show interfaces summary vlan
Total number of Vlan interfaces: 7
Vlan interfaces configured:
1,5,20,2000,3000-3001,4000
Router#
```

This example shows how to display the total number of VLAN interfaces on a Cisco 7600 series router:

```
Router# show interfaces summary vlan
Total number of Vlan interfaces: 7
Vlan interfaces configured:
1,5,20,2000,3000-3001,4000
Router#
```

This example shows how to display a summary of the interfaces on a Cisco 4400 Series Integrated Services Router.

```
#show interfaces summary

 *: interface is up
 IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
 RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
 TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
 TRTL: throttle count

  Interface                  IHQ       IQD       OHQ       OQD      RXBS      RXPS
TXBS      TXPS      TRTL
-----------------------------------------------------------------------------------------

  GigabitEthernet0/0/0         0         0         0         0         0         0
  0         0         0
  GigabitEthernet0/0/1         0         0         0         0         0         0
  0         0         0
  GigabitEthernet0/0/2         0         0         0         0         0         0
  0         0         0
  GigabitEthernet0/0/3         0         0         0         0         0         0
  0         0         0
* Serial1/0/0                  0         0         0         0         0         0
  0         0         0
* GigabitEthernet0             0         0         0         0     31000        60
  0         0         0
```

Related Commands

Command	Description
show interfaces	Displays the statistical information specific to interfaces.
show interfaces atm	Displays information about the ATM interfaces.
show interfaces ethernet	Displays information about the Ethernet interfaces.
show interfaces fastethernet	Displays information about the Fast Ethernet interfaces.
show interfaces serial	Displays information about the serial interfaces.

show interfaces switchport

To display the administrative and operational status of a switching (nonrouting) port, use the **showinterfacesswitchport** command in user EXEC or privileged EXEC mode.

show interfaces [*interface interface-number*] **switchport** [**brief**] [**module** *number*]

Syntax Description

interface	(Optional) Interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **pos**, **atm**, and **ge-wan**.
interface-number	(Optional) Module and port number; see the "Usage Guidelines" section for valid values.
brief	(Optional) Displays a brief summary of information.
module *number*	(Optional) Limits the display to interfaces on a specified module; see the "Usage Guidelines" section for valid values.

Command Default

This command has no default settings.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX	The Administrative Trunking Encapsulation field was changed to dot1q EtherType.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXE	This command was changed to include the **brief** keyword on the Supervisor Engine 720 only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The *interface-number* designates the module and port number. Valid values depend on the chassis and module that are used. For example, if you have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the slot number are from 1 to 13 and valid values for the port number are from 1 to 48.

Examples

This example shows how to display switch-port information using the **include** output modifier:

```
Router>
show interfaces switchport
| include VLAN
Name: Fa5/6
Access Mode VLAN: 200 (VLAN0200)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: ALL
.
.
```

```
.
Router>
```

This example shows how to display the configurations of two multiple VLAN access ports:

```
Router>
show interfaces switchport
Name: Fa5/1
Switchport: Enabled
Administrative Mode: access
Operational Mode: access
Dot1q Ethertype: 0x8200
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: off
Access Mode VLAN: 100
Voice VLAN: 102
Trunking Native Mode VLAN: 1 (default)
Administrative private-vlan host-association: none
Administrative private-vlan mapping: 900 ((Inactive)) 901 ((Inactive))
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Name: Fa5/2
Switchport: Enabled
Administrative Mode: access
Operational Mode: down
Dot1q Ethertype: 0x8200
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 100
Voice VLAN: 103 ((inactive))
Trunking Native Mode VLAN: 1 (default)
.
.
.
```

This example shows how to display a brief summary of information:

```
Router> show interfaces switchport
 brief module 3
Port Status Op.Mode Op.Encap Channel-id Vlan
Fa3/1 connected access native -- 1
Fa3/7 disabled -- dot1q Po26 1
Fa3/13 connected access native -- 666
Router>
```

Related Commands

Command	Description
show interfaces	Displays the status and statistics for the interfaces in the chassis.

show interfaces switchport backup

To display Flexlink pairs, use the **showinterfacesswitchportbackup** command in user EXEC or privileged EXEC mode.

show interfaces [*interface interface-number*] **switchport backup**

Syntax Description

interface	(Optional) Interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **pos**, **atm**, and **ge-wan**.
interface-number	(Optional) Module and port number; see the "Usage Guidelines" section for valid values.

Command Default

This command has no default settings.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(18)SXF	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The *interface-number* designates the module and port number. Valid values depend on the chassis and module that are used. For example, if you have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the slot number are from 1 to 13 and valid values for the port number are from 1 to 48.

Examples

This example shows how to display all Flexlink pairs:

```
Router> show interfaces switchport backup
Switch Backup Interface Pairs:
Active Interface        Backup Interface        State
------------------------------------------------------------------------
FastEthernet3/1         FastEthernet4/1         Active Up/Backup Standby
FastEthernet5/1         FastEthernet5/2         Active Down/Backup Up
FastEthernet3/2         FastEthernet5/4         Active Standby/Backup Up
Po1                     Po2                     Active Down/Backup Down
Router>
```

This example shows how to display a specific Flexlink port:

```
Router> show interfaces fastethernet 4/1 switchport backup
Switch Backup Interface Pairs:
Active Interface        Backup Interface        State
------------------------------------------------------------------------
FastEthernet3/1       FastEthernet4/1           Active Up/Backup Standby
Router>
```

Related Commands

Command	Description
switchport backup	Configures an interface as a Flexlink backup interface.

show interfaces tokenring

To display information about the Token Ring interface and the state of source route bridging, use the **showinterfacestokenring** command in privileged EXEC mode.

Standard Syntax
show interfaces tokenring *number* [**accounting**]

Cisco 7200 and Cisco 7500 Series
show interfaces tokenring *slot/port* [**accounting**]

Cisco 7500 Series with Ports on VIPs
show interfaces tokenring [*slot/port-adapter/port*]

Syntax Description

number	Interface port line number.
accounting	(Optional) Displays the number of packets of each protocol type that have been sent through the interface.
slot	On the Cisco 7000 series routers, slot location of the interface processor. On the Cisco 7000, the value can be 0, 1, 2, 3, or 4. On the Cisco 7010, the value can be 0, 1, or 2. On the Cisco 7200 series routers, slot location of the port adapter; the value can be 1, 2, 3, 4, 5, or 6.
/ *port*	Port number on the interface. On the Cisco 7000 series routers this argument is required, and the values can be 0, 1, 2, or 3. (Optional) For the VIP, this argument is optional, and the port value can be 0, 1, 2, or 3 for 4-port Token Ring interfaces. On the Cisco 7200 series routers, the number depends on the type of port adapter installed.
/ *port-adapter*	(Optional) On the Cisco 7000 series and Cisco 7500 series routers, specifies the ports on a VIP. The value can be 0 or 1.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
11.3(3)T	The information was modified to include the PA-4R-FDX full-duplex Token Ring port adapter.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If you do not provide values for the *slot* and *port*arguments, the command displays statistics for all the network interfaces. The optional **accounting** keyword displays the number of packets of each protocol type that have been sent through the interface.

Examples

The following is sample output from the **showinterfacestokenring** command:

```
Router# show interfaces tokenring
TokenRing 0 is up, line protocol is up
Hardware is 16/4 Token Ring, address is 5500.2000.dc27 (bia 0000.3000.072b)
    Internet address is 10.136.230.203, subnet mask is 255.255.255.0
    MTU 8136 bytes, BW 16000 Kbit, DLY 630 usec, rely 255/255, load 1/255
    Encapsulation SNAP, loopback not set, keepalive set (10 sec)
    ARP type: SNAP, ARP Timeout 4:00:00
    Ring speed: 16 Mbps
    Single ring node, Source Route Bridge capable
    Group Address: 0x00000000, Functional Address: 0x60840000
    Last input 0:00:01, output 0:00:01, output hang never
    Output queue 0/40, 0 drops; input queue 0/75, 0 drops
    Five minute input rate 0 bits/sec, 0 packets/sec
    Five minute output rate 0 bits/sec, 0 packets/sec
    16339 packets input, 1496515 bytes, 0 no buffer
          Received 9895 broadcasts, 0 runts, 0 giants
          0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     32648 packets output, 9738303 bytes, 0 underruns
0 output errors, 0 collisions, 2 interface resets, 0 restarts
     5 transitions
```

The table below describes the significant fields shown in the displays.

Table 160: show interfaces tokenring Field Descriptions

Field	Description
Token Ring is {up | down}	Interface is either currently active and inserted into ring (up) or inactive and not inserted (down). On the Cisco 7500 series routers, gives the interface processor type, slot number, and port number.
Token Ring is Reset	Hardware error has occurred.
Token Ring is Initializing	Hardware is up, in the process of inserting the ring.
Token Ring is Administratively Down	Hardware has been taken down by an administrator.
line protocol is {up | down | administratively down}	Indicates whether the software processes that handle the line protocol believe the interface is usable (that is, whether keepalives are successful).
Hardware	Hardware type. “Hardware is Token Ring” indicates that the board is a CSC-R board. “Hardware is 16/4 Token Ring” indicates that the board is a CSC-R16 board. Also shows the address of the interface.
Internet address	Lists the Internet address followed by subnet mask.
MTU	Maximum transmission unit of the interface.

Field	Description
BW	Bandwidth of the interface, in kilobits per second.
DLY	Delay of the interface, in microseconds.
rely	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method assigned to interface.
loopback	Indicates whether loopback is set or not.
keepalive	Indicates whether keepalives are set or not.
ARP type	Type of Address Resolution Protocol assigned.
Ring speed	Speed of Token Ring--4 or 16 Mbps.
{Single ring | multiring node}	Indicates whether a node is enabled to collect and use source routing information (RIF) for routable Token Ring protocols.
Group Address	Interface's group address, if any. The group address is a multicast address; any number of interfaces on the ring may share the same group address. Each interface may have at most one group address.
Functional Address:	Bit-significant group address. Each "on" bit represents a function performed by the station.
Ethernet Transit OUI:	The Organizational Unique Identifier (OUI) code to be used in the encapsulation of Ethernet Type II frames across Token Ring backbone networks.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This counter is updated only when packets are process-switched, not when packets are fast-switched.
Last output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by an interface. This counter is updated only when packets are process-switched, not when packets are fast-switched.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.

Field	Description
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. *** indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 231 ms (and less than 232 ms) ago.
Output queue, drops Input queue, drops	Number of packets in output and input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped because of a full queue.
Five minute input rate, Five minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes. The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.
packets input	Total number of error-free packets received by the system.
bytes input	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernet networks and bursts of noise on serial lines are often responsible for no input buffer events.
broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium.
giants	Number of packets that are discarded because they exceed the of them medium maximum packet size.
CRC	Cyclic redundancy checksum generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of a station transmitting bad data.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets.
overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.

Field	Description
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be increased.
packets output	Total number of messages transmitted by the system.
bytes output	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the far-end transmitter has been running faster than the near-end router's receiver can handle. This may never be reported on some interfaces.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors, as some datagrams may have more than one error, and others may have errors that do not fall into any of the specifically tabulated categories.
collisions	Since a Token Ring cannot have collisions, this statistic is nonzero only if an unusual event occurred when frames were being queued or dequeued by the system software.
interface resets	Number of times an interface has been reset. The interface may be reset by the administrator or automatically when an internal error occurs.
restarts	Should always be zero for Token Ring interfaces.
transitions	Number of times the ring made a transition from up to down, or vice versa. A large number of transitions indicates a problem with the ring or the interface.

The following is sample output from the **showinterfacestokenring** command on a Cisco 7500 series routers:

```
Router# show interfaces tokenring 2/0
TokenRing2/0 is administratively down, line protocol is down
  Hardware is cxBus Token Ring, address is 0000.3040.8b4a (bia 0000.3040.8b4a)
  MTU 8136 bytes, BW 16000 Kbit, DLY 630 usec, rely 255/255, load 1/255
  Encapsulation SNAP, loopback not set, keepalive set (10 sec)
  ARP type: SNAP, ARP Timeout 4:00:00
  Ring speed: 0 Mbps
  Single ring node, Source Route Transparent Bridge capable
  Ethernet Transit OUI: 0x0000F8
  Last input never, output never, output hang never
  Last clearing of “show interface” counters never
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  Five minute input rate 0 bits/sec, 0 packets/sec
  Five minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
```

```
     0 output errors, 0 collisions, 1 interface resets, 0 restarts
     1 transitions
```

The following example on the Cisco 7500 series routers includes the **accounting** option. When you use the accounting option, only the accounting statistics are displayed.

```
Router# show interfaces tokenring 2/0 accounting
TokenRing2/0
       Protocol    Pkts In   Chars In   Pkts Out  Chars Out
             IP       7344    4787842       1803    1535774
      Appletalk      33345    4797459      12781    1089695
        DEC MOP          0          0        127       9779
            ARP          7        420         39       2340
```

The table below describes thefields shown in the display.

*Table 161: **show interfaces tokenring** Field Descriptions--Accounting*

Field	Description
Protocol	Protocol that is operating on the interface.
Pkts In	Number of packets received for that protocol.
Chars In	Number of characters received for that protocol.
Pkts Out	Number of packets transmitted for that protocol.
Chars Out	Number of characters transmitted for that protocol.

show interfaces transceiver

To display information about the optical transceivers that have digital optical monitoring (DOM) enabled, use the **showinterfacestransceiver** command in privileged EXEC mode.

Catalyst 6500 Series Switches and Cisco 7600 Series Routers
show interfaces [*interface interface-number*] **transceiver** [{**threshold violations** | **properties**}] [{**detail** | **module** *number*}]

Cisco 7200 VXR
show interfaces [*interface interface-number*] **transceiver**

Cisco ASR 901 Routers
show interfaces [*interface interface-number*] **transceiver** [{**threshold** {**table** | **violations**} | **detail** | **supported-list**}]

Cisco ASR 1000 Routers
show interfaces transceiver

Syntax Description

interface	(Optional) Interface type; possible valid values are **gigabitethernet** and **tengigabitethernet**.
interface-number	Module and port number; see the "Usage Guidelines" section for valid values.
threshold violations	(Optional) Displays information about the interface transceiver threshold violations.
properties	(Optional) Displays information about the port speed and duplex autonegotiation status.
detail	(Optional) Displays detailed information about the interface transceiver.
module *number*	(Optional) Specifies the module number; see the "Usage Guidelines" section for valid values.
threshold {**table** | **violations**}	(Optional) Displays information about the transceiver threshold. • **table**—Displays the alarm and warning threshold table. • **violations**—Displays the alarm and warning threshold violations.
supported-list	(Optional) Displays a list of all supported DOM transceivers.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(17d)SXB2	Support for this command was introduced on the Supervisor Engine 720 and the Supervisor Engine 2.
12.2(18)SXE	This command was changed to support DOM for GBICs and XENPAKs.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T for the Cisco 7200 VXR with the NPE-G2 network processing engine.
12.2(33)SXI	This command was changed to display the port speed and duplex autonegotiation status
15.2(2)SNI	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.
Cisco IOS XE Gibraltar 16.10.1	This command was implemenred on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

After a transceiver is inserted, the software waits approximately 10 seconds before reading the diagnostic monitoring information. If you enter the **showinterfacestransceiver** command before the software has read the diagnostic monitoring information, the following message is displayed:

```
Waiting for diagnostic monitoring information to settle down.
Please try again after a few seconds.
```

Wait a few seconds and re-enter the **showinterfacestransceiver** command.

The *interfaceinterface-number* arguments are supported on interfaces that have a transceiver that has diagnostic monitoring enabled and the transceiver is in a module that supports the reading of diagnostic monitoring information. The transceiver periodically polls operating conditions such as temperature and power levels. The show interfaces transceiver command allows the router to display these operating conditions while the transceiver is in service.

Examples

This example shows how to display transceiver information:

```
Router# show interfaces transceiver
If device is externally calibrated, only calibrated values are printed.
++ : high alarm, +  : high warning, -  : low warning, -- : low alarm.
NA or N/A: not applicable, Tx: transmit, Rx: receive.
mA: milliamperes, dBm: decibels (milliwatts).
                                          Optical   Optical
         Temperature  Voltage  Current    Tx Power  Rx Power
Port     (Celsius)    (Volts)  (mA)       (dBm)     (dBm)
-------  -----------  -------  --------   --------  --------
Gi1/1      40.6       5.09       0.4      -25.2      N/A
Gi2/1      35.5       5.05       0.1      -29.2      N/A
Gi2/2      49.5       3.30       0.0        7.1     -18.7
```

This example shows how to display detailed transceiver information:

```
Router# show interfaces transceiver detail
mA: milliamperes, dBm: decibels (milliwatts), NA or N/A: not applicable.
++ : high alarm, +  : high warning, -  : low warning, -- : low alarm.
A2D readouts (if they differ), are reported in parentheses.
The threshold values are calibrated.
```

```
                             High Alarm  High Warn  Low Warn   Low Alarm
        Temperature          Threshold   Threshold  Threshold  Threshold
Port     (Celsius)           (Celsius)   (Celsius)  (Celsius)  (Celsius)
------- ------------------  ----------  ---------  ---------  ---------
Gi1/1     48.1                100.0       100.0        0.0        0.0
Gi1/2     34.9                100.0       100.0        0.0        0.0
Gi2/1     43.5                 70.0        60.0        5.0        0.0
Gi2/2     39.1                 70.0        60.0        5.0        0.0
                             High Alarm  High Warn  Low Warn   Low Alarm
         Voltage             Threshold   Threshold  Threshold  Threshold
Port     (Volts)             (Volts)     (Volts)    (Volts)    (Volts)
-------  ---------------    ----------  ---------  ---------  ---------
Gi1/1    3.30                  6.50        6.50        N/A        N/A
Gi1/2    3.30                  6.50        6.50        N/A        N/A
Gi2/1    5.03                  5.50        5.25       4.75       4.50
Gi2/2    5.02                  5.50        5.25       4.75       4.50
                             High Alarm  High Warn  Low Warn   Low Alarm
         Current             Threshold   Threshold  Threshold  Threshold
Port     (milliamperes)      (mA)        (mA)       (mA)       (mA)
-------  -----------------  ----------  ---------  ---------  ---------
Gi1/1      0.0                130.0       130.0       N/A        N/A
Gi1/2      1.7                130.0       130.0       N/A        N/A
Gi2/1     50.6          +      60.0        40.0       10.0        5.0
Gi2/2     25.8                 60.0        40.0       10.0        5.0
         Optical             High Alarm  High Warn  Low Warn   Low Alarm
         Transmit Power      Threshold   Threshold  Threshold  Threshold
Port     (dBm)               (dBm)       (dBm)      (dBm)      (dBm)
-------  -----------------  ----------  ---------  ---------  ---------
Gi1/1      8.1          ++     8.1         8.1        N/A        N/A
Gi1/2     -9.8                 8.1         8.1        N/A        N/A
Gi2/1    -16.7          --     3.4         3.2       -0.3       -0.5
Gi2/2      0.8                 3.4         3.2       -0.3       -0.5
         Optical             High Alarm  High Warn  Low Warn   Low Alarm
         Receive Power       Threshold   Threshold  Threshold  Threshold
Port     (dBm)               (dBm)       (dBm)      (dBm)      (dBm)
-------  -----------------  ----------  ---------  ---------  ---------
Gi1/1     N/A                  8.1         8.1        N/A        N/A
Gi1/2    -30.9                 8.1         8.1        N/A        N/A
Gi2/1     N/A                  5.9        -6.7      -28.5      -28.5
Gi2/2     N/A                  5.9        -6.7      -28.5      -28.5
```

This example shows how to display the threshold violations for all the transceivers on a Cisco 7600 series router:

```
Router# show interfaces transceiver threshold violations
        Rx: Receive, Tx: Transmit.
        DDDD: days, HH: hours, MM: minutes, SS: seconds
                                Time since Last Known
                Time in slot    Threshold Violation     Type(s) of Last Known
        Port    (DDDD:HH:MM:SS)  (DDDD:HH:MM:SS)        Threshold Violation(s)
        ------- --------------- ----------------------  ----------------------
        Gi1/1    0000:00:03:41    Not applicable        Not applicable
        Gi2/1    0000:00:03:40    0000:00:00:30         Tx bias high warning
                                                         50.5 mA >  40.0 mA
                                  0000:00:00:30         Tx power low alarm
                                                        -17.0 dBm <  -0.5 dBm
        Gi2/2    0000:00:03:40    Not applicable        Not applicable
```

This example shows how to display the threshold violations for all the transceivers on a Catalyst 6500 series switch:

```
Router# show interfaces transceiver threshold violations
        Rx: Receive, Tx: Transmit.
```

```
        DDDD: days, HH: hours, MM: minutes, SS: seconds
                                Time since Last Known
                Time in slot    Threshold Violation     Type(s) of Last Known
        Port    (DDDD:HH:MM:SS)  (DDDD:HH:MM:SS)        Threshold Violation(s)
        ------- --------------- ----------------------  ----------------------
        Gi1/1    0000:00:03:41    Not applicable        Not applicable
        Gi2/1    0000:00:03:40    0000:00:00:30         Tx bias high warning
                                                         50.5 mA >  40.0 mA
                                  0000:00:00:30         Tx power low alarm
                                                        -17.0 dBm <  -0.5 dBm
        Gi2/2    0000:00:03:40    Not applicable        Not applicable
Router#
```

This example shows how to display the threshold violations for all transceivers on a specific module:

```
Router# show interfaces transceiver threshold violations module 2
        lo: low, hi: high, warn: warning
        DDDD: days, HH: hours, MM: minutes, SS: seconds
                                Time since Last Known
                Time in slot    Threshold Violation     Type(s) of Last Known
        Port    (DDDD:HH:MM:SS)  (DDDD:HH:MM:SS)        Threshold Violation
        ------- --------------  ----------------------  ----------------------
        Gi2/1    0000:00:03:40    0000:00:00:30         Tx bias high warning
                                                         50.5 mA >  40.0 mA
                                  0000:00:00:30         Tx power low alarm
                                                        -17.0 dBm <  -0.5 dBm
        Gi2/2    0000:00:03:40    Not applicable        Not applicable
```

This example shows how to display violations for the transceiver on a specific interface:

```
Router# show interfaces Gi2/1 transceiver threshold violations
        Rx: Receive, Tx: Transmit.
        DDDD: days, HH: hours, MM: minutes, SS: seconds
                                Time since Last Known
                Time in slot    Threshold Violation     Type(s) of Last Known
        Port    (DDDD:HH:MM:SS)  (DDDD:HH:MM:SS)        Threshold Violation(s)
        ------- --------------- ----------------------  ----------------------
        Gi2/1    0000:00:03:40    0000:00:00:30         Tx bias high warning
                                                         50.5 mA >  40.0 mA
                                  0000:00:00:30         Tx power low alarm
                                                        -17.0 dBm <  -0.5 dBm
```

This example shows how to display the port speed and duplex autonegotiation status:

```
Router# show interfaces transceiver properties module 1
Name : Fa1/1
Administrative Speed Negotiation: Enable
Administrative Duplex Negotiation: Enable
Name : Fa1/2
Administrative Speed Negotiation: Disable
Administrative Duplex Negotiation: Enable
Name : Fa1/2
Administrative Speed Negotiation: Disable
Administrative Duplex Negotiation: Disable
Router#
```

This example shows how to use the show transceiver command on ASR 1000

```
The Transceiver in slot 1 subslot 0 port 0 is enabled.
Module temperature = +33.238 C [Range: +0.000 to +70.000 C]
Transceiver Tx supply voltage = 3.2942 Volts [Range: 3.1350 to 3.4650 Volts]
Transceiver Tx power = -4.1 dBm
Transceiver Rx optical power = -6.2 dBm
```

```
Tx power Network Lane[00] = -2.3 dBm (0.5824 in units of mW) [Range:-7.6 to -0.5 dBm]
Tx power Network Lane[01] = -2.1 dBm (0.6178 in units of mW) [Range:-7.6 to -0.5 dBm]
Tx power Network Lane[02] = -2.0 dBm (0.6359 in units of mW) [Range:-7.6 to -0.5 dBm]
Tx power Network Lane[03] = -1.9 dBm (0.6531 in units of mW) [Range:-7.6 to -0.5 dBm]
Tx power Network Lane[04] = -2.4 dBm (0.5821 in units of mW) [Range:-7.6 to -0.5 dBm]
Tx power Network Lane[05] = -2.0 dBm (0.6319 in units of mW) [Range:-7.6 to -0.5 dBm]
Tx power Network Lane[06] = -2.0 dBm (0.6268 in units of mW) [Range:-7.6 to -0.5 dBm]
Tx power Network Lane[07] = -1.9 dBm (0.6511 in units of mW) [Range:-7.6 to -0.5 dBm]
Tx power Network Lane[08] = -2.2 dBm (0.6076 in units of mW) [Range:-7.6 to -0.5 dBm]
Tx power Network Lane[09] = -2.1 dBm (0.6153 in units of mW) [Range:-7.6 to -0.5 dBm]
Tx power Network Lane[10] = -40.0 dBm (0.0 in units of mW) [Range:-7.6 to -0.5 dBm]
Tx power Network Lane[11] = -40.0 dBm (0.0 in units of mW) [Range:-7.6 to -0.5 dBm]
Tx power Network Lane[12] = -40.0 dBm (0.0 in units of mW) [Range:-7.6 to -0.5 dBm]
Tx power Network Lane[13] = -40.0 dBm (0.0 in units of mW) [Range:-7.6 to -0.5 dBm]
Tx power Network Lane[14] = -40.0 dBm (0.0 in units of mW) [Range:-7.6 to -0.5 dBm]
Tx power Network Lane[15] = -40.0 dBm (0.0 in units of mW) [Range:-7.6 to -0.5 dBm]
Rx power Network Lane[00] = -4.3 dBm (0.3697 in units of mW) [Range:-9.5 to 2.4 dBm]
Rx power Network Lane[01] = -3.7 dBm (0.4309 in units of mW) [Range:-9.5 to 2.4 dBm]
Rx power Network Lane[02] = -5.3 dBm (0.2959 in units of mW) [Range:-9.5 to 2.4 dBm]
Rx power Network Lane[03] = -3.2 dBm (0.4826 in units of mW) [Range:-9.5 to 2.4 dBm]
Rx power Network Lane[04] = -6.6 dBm (0.2175 in units of mW) [Range:-9.5 to 2.4 dBm]
Rx power Network Lane[05] = -4.0 dBm (0.4012 in units of mW) [Range:-9.5 to 2.4 dBm]
Rx power Network Lane[06] = -3.9 dBm (0.4062 in units of mW) [Range:-9.5 to 2.4 dBm]
Rx power Network Lane[07] = -4.7 dBm (0.3423 in units of mW) [Range:-9.5 to 2.4 dBm]
Rx power Network Lane[08] = -3.5 dBm (0.4444 in units of mW) [Range:-9.5 to 2.4 dBm]
Rx power Network Lane[09] = -3.1 dBm (0.4895 in units of mW) [Range:-9.5 to 2.4 dBm]
Rx power Network Lane[10] = -40.0 dBm (0.0 in units of mW) [Range:-9.5 to 2.4 dBm]
Rx power Network Lane[11] = -40.0 dBm (0.0 in units of mW) [Range:-9.5 to 2.4 dBm]
Rx power Network Lane[12] = -40.0 dBm (0.0 in units of mW) [Range:-9.5 to 2.4 dBm]
Rx power Network Lane[13] = -40.0 dBm (0.0 in units of mW) [Range:-9.5 to 2.4 dBm]
Rx power Network Lane[14] = -40.0 dBm (0.0 in units of mW) [Range:-9.5 to 2.4 dBm]
Rx power Network Lane[15] = -40.0 dBm (0.0 in units of mW) [Range:-9.5 to 2.4 dBm]
Bias Current Network Lane[00] = 6.216 (in units of mA) [Range:0.0 to 43.520 mA]
Bias Current Network Lane[01] = 5.756 (in units of mA) [Range:0.0 to 43.520 mA]
Bias Current Network Lane[02] = 6.304 (in units of mA) [Range:0.0 to 43.520 mA]
Bias Current Network Lane[03] = 6.224 (in units of mA) [Range:0.0 to 43.520 mA]
Bias Current Network Lane[04] = 6.194 (in units of mA) [Range:0.0 to 43.520 mA]
Bias Current Network Lane[05] = 6.84 (in units of mA) [Range:0.0 to 43.520 mA]
Bias Current Network Lane[06] = 6.196 (in units of mA) [Range:0.0 to 43.520 mA]
Bias Current Network Lane[07] = 6.222 (in units of mA) [Range:0.0 to 43.520 mA]
Bias Current Network Lane[08] = 6.208 (in units of mA) [Range:0.0 to 43.520 mA]
Bias Current Network Lane[09] = 5.556 (in units of mA) [Range:0.0 to 43.520 mA]
Bias Current Network Lane[10] = 0.0 (in units of mA) [Range:0.0 to 43.520 mA]
Bias Current Network Lane[11] = 0.0 (in units of mA) [Range:0.0 to 43.520 mA]
Bias Current Network Lane[12] = 0.0 (in units of mA) [Range:0.0 to 43.520 mA]
Bias Current Network Lane[13] = 0.0 (in units of mA) [Range:0.0 to 43.520 mA]
Bias Current Network Lane[14] = 0.0 (in units of mA) [Range:0.0 to 43.520 mA]
Bias Current Network Lane[15] = 0.0 (in units of mA) [Range:0.0 to 43.520 mA]
IDPROM for transceiver HundredGigE1/0/0:
Description = CPAK optics (type 131)
Transceiver Type: = CPAK 100GE SR10 (313)
Product Identifier (PID) = CPAK-100G-SR10
Vendor Revision = 01
Serial Number (SN) = FBN181720831
Vendor Name = CISCO
Vendor OUI (IEEE company ID) = 00.00.0C (12)
CLEI code = WOTRC5PBAA
Cisco part number = 800-41495-
Device State = Enabled.
Date code (yyyy/mm/dd) = 2014/04/24
Connector type = MPO.
Encoding = NRZ, Non-PSK.
Bit Rate = 111.8 Gbps
Maximum Bit Rate Network Lane = 11.2 Gbits/s
```

```
Maximum Bit Rate Host Lane = 11.2 Gbits/s
The Transceiver in slot 1 subslot 1 port 0 is enabled.
Module temperature = +43.578 C [Range: 0 to 70 C]
Transceiver Tx supply voltage = 3287.5 mVolts [Range: 3135.0 to 3465.0 mVolts]
Transceiver Tx bias current = 7710 uAmps [Range: 5000 to 10800 uAmps]
Transceiver Tx power = -2.0 dBm [Range: -7.3 to -1.3 dBm]
Transceiver Rx optical power = -2.0 dBm [Range:-9.9 to -1.0 dBm]
IDPROM for transceiver TenGigabitEthernet1/1/0:
Description = SFP+ optics (type 130)
Transceiver Type: = SFP+ 10GBASE-SR (273)
Product Identifier (PID) = SFP-10G-SR
Vendor Revision = A
Serial Number (SN) = FNS173814XB
Vendor Name = CISCO-FINISAR
Vendor OUI (IEEE company ID) = 00.90.65 (36965)
CLEI code = COUIA8NCAA
Cisco part number = 10-2415-03
Device State = Enabled.
Date code (yy/mm/dd) = 13/09/17
Connector type = LC.
Encoding = 64B66B
Nominal bitrate = 10GE (10300 Mbits/s)
Minimum bit rate as % of nominal bit rate = not specified
Maximum bit rate as % of nominal bit rate = not specified
```

Cisco ASR 901 Routers

show interfaces [*interface interface-number*] **transceiver** [{**threshold** {**table** | **violations**} | **detail** | **supported-list**}]

Cisco 7200 VXR

This example shows static information and current status information for the transceiver. The static information is a description of the transceiver and its physical capabilities, which is provided by the manufacturer in EEPROM. The status information shows current operating conditions, as well as alarm and warning threshold ranges.

Alarms indicate conditions that might be associated with a non-operational link and are cause for immediate action. Warnings indicate conditions outside the normally guaranteed ranges but are not necessarily causes of immediate link failures. Certain warnings can also be defined by the manufacturer as end-of-life indicators, such as higher than expected bias currents in a constant power control loop.

In this example, the fiber optic cable is disconnected and the appropriate alarms and warnings are displayed.

```
Router# show interfaces g0/3 transceiver
Static information
  ID: SFP transceiver
  Extended ID: 4
  Connector: LC
  SONET compliance: unspecified
  Gigabit Ethernet compliance: 1000BASE-SX
  Fibre Channel link length: unspecified
  Fibre Channel transmitter technology: unspecified
  Fibre Channel transmission media: unspecified
  Fibre Channel speed: unspecified
  Encoding: 8B10B
  Bit Rate: 1300 Mbps
  50 micron-multimode fiber supported length: 550 m
```

```
  62.5 micron-multimode fiber supported length: 270 m
  Upper bit rate limit: unspecified
  Lower bit rate limit: unspecified
  Date code (yyyy/mm/dd): 2005/03/21
  Vendor PN: FTRJ8519P1BNL-C6
  Vendor revision number: A
  Vendor serial number: FNS0913D1HL
Transceiver status information
  Diagnostics calibration is external
  Temperature 36 (+/-3 Celsius)
  Voltage in transceiver 3320000 uV (+/- 10 mV)
  TX bias 260 uA (+/- 100uA)
  TX power 700 nW / -31 dBm (+/- 3dBm)
  RX power (No signal detected: fiber might be bad or disconnected).
UDI(PID + VID + SN):FNS0913D1HL
Alarms
  TX power low
  TX bias low
  RX power low
Warnings
  TX power low
  TX bias low
  RX power low
Alarm Thresholds:
                       high                           low
Temperature             109 C                         -29 C
Voltage             3900000 uV                    2700000 uV
TX bias               15000 uA                       1000 uA
TX power             629700 nW /-2 dBm              49800 nW / -13 dBm
RX power              1258900 nW / 0 dBm                10000 nW / -20 dBm
Warning Thresholds:
                       high                           low
Temperature             103 C                         -13 C
Voltage             3700000 uV                    2900000 uV
TX bias               12000 uA                       2000 uA
TX power             629700 nW / -2 dBm             78800 nW / -11 dBm
RX power               794000 nW / -1 dBm               15800 nW / -18 dBm
```

The table below describes the significant fields shown in the display.

Table 162: show interfaces transceiver Field Descriptions

Field	Description
Diagnostics calibration	Indicates whether diagnostic information (temperature, voltage, bias, and power) is calibrated internally or externally. Internal calibration means that measurements are calibrated over vendor-specified operating temperature and voltage. External calibration means that measurements are raw analog/digital values and are converted to common units of measure, such as volts and amperes, using calibration constants stored in EEPROM.
Temperature	Internally-measured transceiver temperature.
Voltage in transceiver	Internally-measured supply voltage.
TX bias	Measured transmitter laser bias current.
TX power	Measured coupled transmit output power.
RX power	Measured received optical power.

Field	Description
UDI	Unique device identifier.

show interfaces transceiver details

The show interfaces transceiver details command displays combined results of **show hw-mod subslot transceiver idprom brief** and **show hw-mod sub transceiver idprom dump** commands. The output also includes error optics information from the line card console and information is displayed for all the transceivers in the router. The output also includes alarm status if CPAK transceivers are installed in the router..

show interfaces transceiverdetails

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Examples

The following is the sample output from the **show interfaces transceiver details** command:.

```
Router# show interfaces transceiver details
IDPROM for transceiver HundredGigE1/0/0:
Description = CPAK optics (type 131)
Transceiver Type: = CPAK 100GE SR10 (313)
Product Identifier (PID) = CPAK-100G-SR10
Vendor Revision = 01
Serial Number (SN) = FBN181720831
Vendor Name = CISCO
Vendor OUI (IEEE company ID) = 00.00.0C (12)
CLEI code = WOTRC5PBAA
Cisco part number = 800-41495-
Device State = Enabled.
Date code (yyyy/mm/dd) = 2014/04/24
Connector type = MPO.
Encoding = NRZ, Non-PSK.
Bit Rate = 111.8 Gbps
Maximum Bit Rate Network Lane = 11.2 Gbits/s
Maximum Bit Rate Host Lane = 11.2 Gbits/s
Phased Initialization
Phase Reached: 5
Phase Exit Code: Success 0
Phase Read Offset: 0x80
Socket Verification
Compatibility: Compatibility passed
Security: Security passed
Idprom Contents (hex)
(CPAK NVR1 Table - addr 0x8000-0x807F)
000: 01 21 09 03 00 00 00 00 1E AA
010: 4A 38 38 00 0A 00 0A 01 83 40
020: 86 60 00 00 00 04 40 50 26 17
030: 14 46 00 43 49 53 43 4F 20 20
040: 20 20 20 20 20 20 20 20 20 00
050: 00 0C 38 30 30 2D 34 31 34 39
060: 35 2D 30 31 20 20 20 20 46 42
070: 4E 31 38 31 37 32 30 38 33 31
080: 20 20 20 20 32 30 31 34 30 34
090: 32 34 00 00 57 4F 54 52 43 35
```

```
100: 50 42 41 41 6E 5A 00 05 02 03
110: 0C 03 0F 20 01 01 08 00 FE 01
120: 00 00 00 02 03 00 00 FC
Threshold Data (hex)
CPAK NVR2 Table - address 0x8080-0x80FF
000: 4B 00 46 00 00 00 FB 00 8A 00
010: 87 5A 7A 76 77 E2 00 00 00 00
020: 00 00 00 00 00 00 00 00 00 00
030: 00 00 00 00 00 00 00 00 00 00
040: 13 88 11 94 05 DC 03 E8 45 76
050: 22 D0 06 C9 03 66 5A 00 55 00
060: 00 00 FB 00 88 71 43 E2 04 62
070: 02 32 00 00 00 00 00 00 00 00
080: 00 00 00 00 00 00 00 00 00 00
090: 00 00 00 00 00 00 00 00 00 00
100: 00 00 00 00 00 00 00 00 00 00
110: 00 00 00 00 00 00 00 00 00 00
120: 00 00 00 00 00 00 00 93
Vendor Idprom Contents (hex)
Vendor Cisco NVR1 Table - address 0x8400-0x847F
000: 02 00 00 00 00 00 00 00 00 00
010: 00 00 00 00 00 00 43 49 53 43
020: 4F 20 20 20 20 20 20 20 20 20
030: 20 20 43 50 41 4B 2D 31 30 30
040: 47 2D 53 52 31 30 20 20 56 45
050: 53 31 07 46 42 4E 31 38 31 37
060: 32 30 38 33 38 30 30 2D 34 31
070: 34 39 35 2D 30 31 30 31 20 20
080: 00 00 00 00 00 00 00 00 00 00
090: 00 32 38 2D 31 31 30 32 30 2D
100: 30 34 00 00 00 00 00 00 00 00
110: 00 00 00 00 00 00 00 00 00 00
120: 00 00 00 00 00 00 00 1B
Vendor Idprom Contents 2 (hex)
Vendor CISCO NVR2 Table - address 0x8480-0x84FF
000: 00 00 00 00 00 00 00 00 00 00
010: 00 00 00 00 00 00 00 00 00 00
020: 00 00 00 00 00 00 00 00 00 00
030: 00 00 41 46 45 30 34 30 46 52
040: 20 20 20 20 20 20 20 20 41 46
050: 45 30 34 42 47 55 20 20 20 20
060: 20 20 20 20 00 00 00 00 00 00
070: 00 00 00 00 00 00 00 00 00 00
080: 53 52 31 34 34 30 31 30 37 39
090: 2D 30 36 20 20 20 00 00 00 00
100: 00 00 00 00 00 00 00 00 00 00
110: 00 00 00 00 00 00 00 00 00 00
120: 00 00 00 00 00 00 00 38
Module State Register: 0x0020
Module General Control Register: 0x0000
Global Alarm Status: 0x0000
Network Lanes Alarm and Warning Status: 0x0000
Network Lanes Fault Status Summary: 0x0000
Host Lanes Fault Status Summary: 0x0000
Module Fault and Warning, General Status Summary: 0x0002
Module Fault and Warning, Fault Status Summary: 0x0000
Fault and Warning status, Alarms and Warning 1: 0x0000
Multimode fiber supported length = 100 m
Enhanced options implemented:
Host Lane PRBS Supported
Enhanced options 2 implemented:
none
Diagnostic monitoring implemented:
Transmitted power measurement type
```

```
Received power measurement type
Diagnostic monitoring capability 1:
Transceiver temperature monitor
Transceiver power supply voltage monitor
Diagnostic monitoring capability 2:
Network Lane laser temperature monitor
Network Lane laser bias current monitor
Network Lane laser output power monitor
Network Lane received power monitor
```

show interfaces transceiver slot

The show interfaces transceiver slot command displays combined results of **show hw-module subslot transceiver status** and show hw-module subslot transceiver idprom brief commands along with the threshold range details. The output is displayed for the transceivers in a specific slot on the router.

show interfaces transceiver slot[{*slot-number*}]

Syntax Description

slot-number	Chassis slot-number.

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Examples

The following is sample output from the **show interfaces transceiver slot** comman::

```
Router# show interfaces transceiver slot 2The Transceiver in slot 2 subslot 0 port 0 is
enabled.
Module temperature = +31.714 C [Range: -5 C to 85 C (extended)]
Transceiver Tx supply voltage = 3331.8 mVolts [Range: 3140.0 to 3470.0 mVolts]
Transceiver Tx bias current = 3112 uAmps [Range: 2400 to 11900 uAmps]
Transceiver Tx power = -5.8 dBm [Range: -9.5 to -3.0 dBm]
Transceiver Rx optical power = -7.4 dBm [Range: -17.0 to 0.0 dBm]
IDPROM for transceiver GigabitEthernet2/0/0:
Description = SFP or SFP+ optics (type 3)
Transceiver Type: = GE SX (19)
Product Identifier (PID) = GLC-SX-MMD
Vendor Revision = 001
Serial Number (SN) = AGJ1825R57R
Vendor Name = CISCO
Vendor OUI (IEEE company ID) = 00.17.6A (5994)
CLEI code = WOTRB9VBAA
Cisco part number = 10-2626-01
Device State = Enabled.
Date code (yy/mm/dd) = 14/06/17
Connector type = LC.
Encoding = 8B10B (1)
Nominal bitrate = GE (1300 Mbits/s)
Minimum bit rate as % of nominal bit rate = not specified
Maximum bit rate as % of nominal bit rate = not specified
```

show interfaces transceiver slot details

The show interfaces transceiver slot details command displays combined results of **show hw-mod subslot transceiver idprom brief** and **show hw-mod sub transceiver idprom dump commands**. The output also includes error optics information from the line card console and information is displayed for all the transceivers in a specific slot. The output also includes alarm details for the CPAK transceivers installed on the router.

show interfaces transceiver slot[{*slot-number*}]**details**

Syntax Description

slot-number	Chassis slot-number.

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Examples

The following is sample output from the **show interfaces transceiver slot details** comman::

```
Router# show interfaces transceiver slot 2 details
IDPROM for transceiver GigabitEthernet2/0/0:
Description = SFP or SFP+ optics (type 3)
Transceiver Type: = GE SX (19)
Product Identifier (PID) = GLC-SX-MMD
Vendor Revision = 001
Serial Number (SN) = AGJ1825R57R
Vendor Name = CISCO
Vendor OUI (IEEE company ID) = 00.17.6A (5994)
CLEI code = WOTRB9VBAA
Cisco part number = 10-2626-01
Device State = Enabled.
Date code (yy/mm/dd) = 14/06/17
Connector type = LC.
Encoding = 8B10B (1)
Nominal bitrate = GE (1300 Mbits/s)
Minimum bit rate as % of nominal bit rate = not specified
Maximum bit rate as % of nominal bit rate = not specified
Phased Initialization
Phase Reached: 5
Phase Exit Code: Success 0
Phase Read Offset: 0x100
Socket Verification
Compatibility: Compatibility passed
Security: Security passed
SFP IDPROM Page 0xA0:
000: 03 04 07 00 00 00 01 00 00 00
010: 00 01 0D 00 00 00 37 1B 00 00
020: 43 49 53 43 4F 20 20 20 20 20
030: 20 20 20 20 20 20 00 00 17 6A
040: 53 46 42 52 2D 35 37 31 36 50
050: 5A 20 20 20 20 20 30 30 31 20
060: 03 52 00 3E 00 1A 00 00 41 47
070: 4A 31 38 32 35 52 35 37 52 20
080: 20 20 20 20 31 34 30 36 31 37
090: 20 20 68 F0 03 3A 00 00 06 BC
100: 13 7F 4C 09 FD 98 52 53 B6 88
```

```
110: B7 DF 55 30 D9 00 00 00 00 00
120: 00 00 00 00 5A 53 74 66 00 00
130: 00 00 00 00 00 00 00 00 00 00
140: 00 00 00 00 00 00 00 00 00 00
150: 00 00 00 00 00 00 00 00 00 00
160: 00 00 00 00 00 00 00 00 00 00
170: 00 00 00 00 00 00 00 00 00 00
180: 00 00 00 00 00 00 00 00 00 00
190: 00 00 00 00 00 00 00 00 00 00
200: 00 00 00 00 00 00 00 00 00 00
210: 00 00 00 00 00 00 00 00 00 00
220: 00 00 00 00
SFP IDPROM Page 0xA2:
000: 5A 00 F6 00 55 00 FB 00 8D CC
010: 74 04 87 8C 7A A8 18 E7 03 E8
020: 17 3E 04 B0 27 10 01 BF 13 94
030: 04 62 4D F0 00 4F 27 10 00 C7
040: 00 00 00 00 00 00 00 00 00 00
050: 00 00 00 00 00 00 00 00 00 00
060: 00 00 00 00 00 00 00 00 3F 80
070: 00 00 00 00 00 00 01 00 00 00
080: 01 00 00 00 01 00 00 00 01 00
090: 00 00 68 00 00 52 1A 1B 82 C1
100: 00 01 00 01 00 01 00 00 00 0F
110: 82 00 05 40 00 00 05 40 00 00
120: 00 00 00 00 00 00 00 01 57 4F
130: 54 52 42 39 56 42 41 41 31 30
140: 2D 32 36 32 36 2D 30 31 56 30
150: 31 20 88 FB 55 00 00 00 00 7C
160: 00 00 00 00 00 00 00 00 00 00
170: 00 00 00 00 00 00 00 00 00 00
180: 00 00 00 00 00 00 00 00 00 00
190: AA AA 47 4C 43 2D 53 58 2D 4D
200: 4D 44 20 20 20 20 20 20 20 20
210: 20 20 00 00 00 00 00 00 00 00
220: 00 00 00 F9 00 00 00 00 00 00
230: 00 00 00 00 00 00 00 00 00 00
240: 00 00 00 00 00 00 00 00 FF FF
250: FF FF 00 00 00 00
Link reach for 9u fiber (km) = SX(550/270m) (0)
1xFC-MM(500/300m) (0)
2xFC-MM(300/150m) (0)
ESCON-MM(2km) (0)
Link reach for 9u fiber (m) = SX(550/270m) (0)
1xFC-MM(500/300m) (0)
2xFC-MM(300/150m) (0)
ESCON-MM(2km) (0)
Link reach for 50u fiber (m) = SX(550/270m) (55)
LX(5km/550m) (55)
LX(10km/550m) (55)
Nominal laser wavelength = 850 nm.
DWDM wavelength fraction = 850.0 nm.
Supported options = Tx disable
Tx fault signal
Loss of signal (standard implementation)
Supported enhanced options = Alarms for monitored parameters
Software Tx disable
Software Tx fault monitoring
Software Rx LOS monitoring
Diagnostic monitoring = Digital diagnostics supported
Diagnostics are internally calibrated
Rx power measured is "Average power"
```

show interfaces transceiver subslot

The **show interfaces transceiver subslot** command displays results of **show hw-module subslot transceiver status** and **show hw-module subslot transceiver idprom brief** command along with threshold range details. The output is displayed for the transceivers in a specific subslot.

show interfaces transceiver subslot[{*subslot-number*}]

Syntax Description

subslot-number	Secondary slot number on a SIP where a SPA is installed..

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Examples

The following is sample output from the **show interfaces transceiver subslot** command:

```
Router# show interfaces transceiver subslot 2/0
The Transceiver in slot 2 subslot 0 port 0 is enabled.
Module temperature = +31.714 C [Range: -5 C to 85 C (extended)]
Transceiver Tx supply voltage = 3331.8 mVolts [Range: 3140.0 to 3470.0 mVolts]
Transceiver Tx bias current = 3112 uAmps [Range: 2400 to 11900 uAmps]
Transceiver Tx power = -5.8 dBm [Range: -9.5 to -3.0 dBm]
Transceiver Rx optical power = -7.4 dBm [Range: -17.0 to 0.0 dBm]
IDPROM for transceiver GigabitEthernet2/0/0:
Description = SFP or SFP+ optics (type 3)
Transceiver Type: = GE SX (19)
Product Identifier (PID) = GLC-SX-MMD
Vendor Revision = 001
Serial Number (SN) = AGJ1825R57R
Vendor Name = CISCO
Vendor OUI (IEEE company ID) = 00.17.6A (5994)
CLEI code = WOTRB9VBAA
Cisco part number = 10-2626-01
Device State = Enabled.
Date code (yy/mm/dd) = 14/06/17
Connector type = LC.
Encoding = 8B10B (1)
Nominal bitrate = GE (1300 Mbits/s)
Minimum bit rate as % of nominal bit rate = not specified
Maximum bit rate as % of nominal bit rate = not specified
```

show interfaces transceiver subslot details

The **show interfaces transceiver subslot details** command displays combined results of **show hw-mod subslot idprom brief** and **show hw-mod subslot idprom dump** commands. The output also includes error optics information from the line card console and information for all the transceivers in a specific subslot. The output also includes alarm details for the CPAK transceivers installed on the router.

show interfaces transceiver subslot[{*subslot-number*}]**details**

Syntax Description

subslot-number	Secondary slot number on a SIP where a SPA is installed..

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Examples

The following is sample output from the **show interfaces transceiver subslot details** command:

```
Router# show interfaces transceiver subslot 2/0 details
IDPROM for transceiver GigabitEthernet2/0/0:
Description = SFP or SFP+ optics (type 3)
Transceiver Type: = GE SX (19)
Product Identifier (PID) = GLC-SX-MMD
Vendor Revision = 001
Serial Number (SN) = AGJ1825R57R
Vendor Name = CISCO
Vendor OUI (IEEE company ID) = 00.17.6A (5994)
CLEI code = WOTRB9VBAA
Cisco part number = 10-2626-01
Device State = Enabled.
Date code (yy/mm/dd) = 14/06/17
Connector type = LC.
Encoding = 8B10B (1)
Nominal bitrate = GE (1300 Mbits/s)
Minimum bit rate as % of nominal bit rate = not specified
Maximum bit rate as % of nominal bit rate = not specified
Phased Initialization
Phase Reached: 5
Phase Exit Code: Success 0
Phase Read Offset: 0x100
Socket Verification
Compatibility: Compatibility passed
Security: Security passed
SFP IDPROM Page 0xA0:
000: 03 04 07 00 00 00 01 00 00 00
010: 00 01 0D 00 00 00 37 1B 00 00
020: 43 49 53 43 4F 20 20 20 20 20
030: 20 20 20 20 20 20 00 00 17 6A
040: 53 46 42 52 2D 35 37 31 36 50
050: 5A 20 20 20 20 20 30 30 31 20
060: 03 52 00 3E 00 1A 00 00 41 47
070: 4A 31 38 32 35 52 35 37 52 20
080: 20 20 20 20 31 34 30 36 31 37
090: 20 20 68 F0 03 3A 00 00 06 BC
100: 13 7F 4C 09 FD 98 52 53 B6 88
```

```
110: B7 DF 55 30 D9 00 00 00 00 00
120: 00 00 00 00 5A 53 74 66 00 00
130: 00 00 00 00 00 00 00 00 00 00
140: 00 00 00 00 00 00 00 00 00 00
150: 00 00 00 00 00 00 00 00 00 00
160: 00 00 00 00 00 00 00 00 00 00
170: 00 00 00 00 00 00 00 00 00 00
180: 00 00 00 00 00 00 00 00 00 00
190: 00 00 00 00 00 00 00 00 00 00
200: 00 00 00 00 00 00 00 00 00 00
210: 00 00 00 00 00 00 00 00 00 00
220: 00 00 00 00
SFP IDPROM Page 0xA2:
000: 5A 00 F6 00 55 00 FB 00 8D CC
010: 74 04 87 8C 7A A8 18 E7 03 E8
020: 17 3E 04 B0 27 10 01 BF 13 94
030: 04 62 4D F0 00 4F 27 10 00 C7
040: 00 00 00 00 00 00 00 00 00 00
050: 00 00 00 00 00 00 00 00 00 00
060: 00 00 00 00 00 00 00 00 3F 80
070: 00 00 00 00 00 00 01 00 00 00
080: 01 00 00 00 01 00 00 00 01 00
090: 00 00 68 00 00 52 1A 1B 82 C1
100: 00 01 00 01 00 01 00 00 00 0F
110: 82 00 05 40 00 00 05 40 00 00
120: 00 00 00 00 00 00 00 01 57 4F
130: 54 52 42 39 56 42 41 41 31 30
140: 2D 32 36 32 36 2D 30 31 56 30
150: 31 20 88 FB 55 00 00 00 00 7C
160: 00 00 00 00 00 00 00 00 00 00
170: 00 00 00 00 00 00 00 00 00 00
180: 00 00 00 00 00 00 00 00 00 00
190: AA AA 47 4C 43 2D 53 58 2D 4D
200: 4D 44 20 20 20 20 20 20 20 20
210: 20 20 00 00 00 00 00 00 00 00
220: 00 00 00 F9 00 00 00 00 00 00
230: 00 00 00 00 00 00 00 00 00 00
240: 00 00 00 00 00 00 00 00 FF FF
250: FF FF 00 00 00 00
Link reach for 9u fiber (km) = SX(550/270m) (0)
1xFC-MM(500/300m) (0)
2xFC-MM(300/150m) (0)
ESCON-MM(2km) (0)
Link reach for 9u fiber (m) = SX(550/270m) (0)
1xFC-MM(500/300m) (0)
2xFC-MM(300/150m) (0)
ESCON-MM(2km) (0)
Link reach for 50u fiber (m) = SX(550/270m) (55)
LX(5km/550m) (55)
LX(10km/550m) (55)
Nominal laser wavelength = 850 nm.
DWDM wavelength fraction = 850.0 nm.
Supported options = Tx disable
Tx fault signal
Loss of signal (standard implementation)
Supported enhanced options = Alarms for monitored parameters
Software Tx disable
Software Tx fault monitoring
Software Rx LOS monitoring
Diagnostic monitoring = Digital diagnostics supported
Diagnostics are internally calibrated
Rx power measured is "Average power"
```

show interfaces <interface> transceiver

The **show interfaces <interface> transceiver** command displays combined results of **show hw-module subslot transceiver status** and **show hw-module subslot transceiver idprom brief** commands along with threshold range details. The output is displayed for a specific interface on the router.

show interfaces[{*interface-typeslot/subslot/port*}] **transceiver**

Syntax Description

interface-type	Interface type; possible valid values are pos, atm, ethernet, fastethernet, gigabitethernet, tengigabitethernet, fortygigabitethernet, hundredGigE.
slot	Number of the router slot.
subslot	Secondary slot number on a SIP where a SPA is installed.
port	Port number

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Examples

The following is sample output from the **show interfaces <interface> transceiver** command:

```
Router# show interfaces hundredGigE 1/0/0 transceiver
The Transceiver in slot 1 subslot 0 port 0 is enabled.
Module temperature = +33.238 C [Range: +0.000 to +70.000 C]
Transceiver Tx supply voltage = 3.2967 Volts [Range: 3.1350 to 3.4650 Volts]
Transceiver Tx power = -4.1 dBm
Transceiver Rx optical power = -6.1 dBm
Tx power Network Lane[00] = -2.3 dBm (0.5823 in units of mW) [Range:-7.6 to -0.5 dBm]
Tx power Network Lane[01] = -2.1 dBm (0.6182 in units of mW) [Range:-7.6 to -0.5 dBm]
Tx power Network Lane[02] = -2.0 dBm (0.6332 in units of mW) [Range:-7.6 to -0.5 dBm]
Tx power Network Lane[03] = -1.9 dBm (0.6522 in units of mW) [Range:-7.6 to -0.5 dBm]
Tx power Network Lane[04] = -2.3 dBm (0.5827 in units of mW) [Range:-7.6 to -0.5 dBm]
Tx power Network Lane[05] = -2.0 dBm (0.6324 in units of mW) [Range:-7.6 to -0.5 dBm]
Tx power Network Lane[06] = -2.0 dBm (0.6251 in units of mW) [Range:-7.6 to -0.5 dBm]
Tx power Network Lane[07] = -1.9 dBm (0.6519 in units of mW) [Range:-7.6 to -0.5 dBm]
Tx power Network Lane[08] = -2.2 dBm (0.6070 in units of mW) [Range:-7.6 to -0.5 dBm]
Tx power Network Lane[09] = -2.1 dBm (0.6148 in units of mW) [Range:-7.6 to -0.5 dBm]
Tx power Network Lane[10] = -40.0 dBm (0.0 in units of mW) [Range:-7.6 to -0.5 dBm]
Tx power Network Lane[11] = -40.0 dBm (0.0 in units of mW) [Range:-7.6 to -0.5 dBm]
Tx power Network Lane[12] = -40.0 dBm (0.0 in units of mW) [Range:-7.6 to -0.5 dBm]
Tx power Network Lane[13] = -40.0 dBm (0.0 in units of mW) [Range:-7.6 to -0.5 dBm]
Tx power Network Lane[14] = -40.0 dBm (0.0 in units of mW) [Range:-7.6 to -0.5 dBm]
Tx power Network Lane[15] = -40.0 dBm (0.0 in units of mW) [Range:-7.6 to -0.5 dBm]
Rx power Network Lane[00] = -4.3 dBm (0.3675 in units of mW) [Range:-9.5 to 2.4 dBm]
Rx power Network Lane[01] = -3.6 dBm (0.4325 in units of mW) [Range:-9.5 to 2.4 dBm]
Rx power Network Lane[02] = -5.3 dBm (0.2963 in units of mW) [Range:-9.5 to 2.4 dBm]
Rx power Network Lane[03] = -3.1 dBm (0.4851 in units of mW) [Range:-9.5 to 2.4 dBm]
Rx power Network Lane[04] = -6.6 dBm (0.2183 in units of mW) [Range:-9.5 to 2.4 dBm]
Rx power Network Lane[05] = -4.0 dBm (0.4015 in units of mW) [Range:-9.5 to 2.4 dBm]
Rx power Network Lane[06] = -3.9 dBm (0.4109 in units of mW) [Range:-9.5 to 2.4 dBm]
Rx power Network Lane[07] = -4.6 dBm (0.3431 in units of mW) [Range:-9.5 to 2.4 dBm]
```

```
Rx power Network Lane[08] = -3.5 dBm (0.4448 in units of mW) [Range:-9.5 to 2.4 dBm]
Rx power Network Lane[09] = -3.1 dBm (0.4895 in units of mW) [Range:-9.5 to 2.4 dBm]
Rx power Network Lane[10] = -40.0 dBm (0.0 in units of mW) [Range:-9.5 to 2.4 dBm]
Rx power Network Lane[11] = -40.0 dBm (0.0 in units of mW) [Range:-9.5 to 2.4 dBm]
Rx power Network Lane[12] = -40.0 dBm (0.0 in units of mW) [Range:-9.5 to 2.4 dBm]
Rx power Network Lane[13] = -40.0 dBm (0.0 in units of mW) [Range:-9.5 to 2.4 dBm]
Rx power Network Lane[14] = -40.0 dBm (0.0 in units of mW) [Range:-9.5 to 2.4 dBm]
Rx power Network Lane[15] = -40.0 dBm (0.0 in units of mW) [Range:-9.5 to 2.4 dBm]
Bias Current Network Lane[00] = 6.262 (in units of mA) [Range:0.0 to 43.520 mA]
Bias Current Network Lane[01] = 5.756 (in units of mA) [Range:0.0 to 43.520 mA]
Bias Current Network Lane[02] = 6.304 (in units of mA) [Range:0.0 to 43.520 mA]
Bias Current Network Lane[03] = 6.178 (in units of mA) [Range:0.0 to 43.520 mA]
Bias Current Network Lane[04] = 6.194 (in units of mA) [Range:0.0 to 43.520 mA]
Bias Current Network Lane[05] = 6.84 (in units of mA) [Range:0.0 to 43.520 mA]
Bias Current Network Lane[06] = 6.198 (in units of mA) [Range:0.0 to 43.520 mA]
Bias Current Network Lane[07] = 6.176 (in units of mA) [Range:0.0 to 43.520 mA]
Bias Current Network Lane[08] = 6.160 (in units of mA) [Range:0.0 to 43.520 mA]
Bias Current Network Lane[09] = 5.556 (in units of mA) [Range:0.0 to 43.520 mA]
Bias Current Network Lane[10] = 0.0 (in units of mA) [Range:0.0 to 43.520 mA]
Bias Current Network Lane[11] = 0.0 (in units of mA) [Range:0.0 to 43.520 mA]
Bias Current Network Lane[12] = 0.0 (in units of mA) [Range:0.0 to 43.520 mA]
Bias Current Network Lane[13] = 0.0 (in units of mA) [Range:0.0 to 43.520 mA]
Bias Current Network Lane[14] = 0.0 (in units of mA) [Range:0.0 to 43.520 mA]
Bias Current Network Lane[15] = 0.0 (in units of mA) [Range:0.0 to 43.520 mA]
IDPROM for transceiver HundredGigE1/0/0:
Description = CPAK optics (type 131)
Transceiver Type: = CPAK 100GE SR10 (313)
Product Identifier (PID) = CPAK-100G-SR10
Vendor Revision = 01
Serial Number (SN) = FBN181720831
Vendor Name = CISCO
Vendor OUI (IEEE company ID) = 00.00.0C (12)
CLEI code = WOTRC5PBAA
Cisco part number = 800-41495-
Device State = Enabled.
Date code (yyyy/mm/dd) = 2014/04/24
Connector type = MPO.
Encoding = NRZ, Non-PSK.
Bit Rate = 111.8 Gbps
Maximum Bit Rate Network Lane = 11.2 Gbits/s
Maximum Bit Rate Host Lane = 11.2 Gbits/s
```

show interfaces <interface> transceiver detail

The **show interfaces <interface> transceiver details** command displays combined results of **show hw-mod subslot transceiver idprom brief** and **show hw-mod sub transceiver idprom dump** commands for a specific interface on the router. The output also includes error optics information from the line card console and alarm status, if CPAK transceivers are installed in the router.

show interfaces[{*interface-typeslot/subslot/port*}] **transceiver detail**

Syntax Description

interface-type	Interface type; possible valid values are pos, atm, ethernet, fastethernet, gigabitethernet, tengigabitethernet, fortygigabitethernet, hundredGigE.
slot	Number of the router slot.
subslot	Secondary slot number on a SIP where a SPA is installed.
port	Port number

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Examples

The following is sample output from the **show interfaces <interface> transceiver detail** command:

```
Router# show interfaces hundredGigE 1/0/0 transceiver
IDPROM for transceiver HundredGigE1/0/0:
Description = CPAK optics (type 131)
Transceiver Type: = CPAK 100GE SR10 (313)
Product Identifier (PID) = CPAK-100G-SR10
Vendor Revision = 01
Serial Number (SN) = FBN181720831
Vendor Name = CISCO
Vendor OUI (IEEE company ID) = 00.00.0C (12)
CLEI code = WOTRC5PBAA
Cisco part number = 800-41495-
Device State = Enabled.
Date code (yyyy/mm/dd) = 2014/04/24
Connector type = MPO.
Encoding = NRZ, Non-PSK.
Bit Rate = 111.8 Gbps
Maximum Bit Rate Network Lane = 11.2 Gbits/s
Maximum Bit Rate Host Lane = 11.2 Gbits/s
Phased Initialization
Phase Reached: 5
Phase Exit Code: Success 0
Phase Read Offset: 0x80
Socket Verification
Compatibility: Compatibility passed
Security: Security passed
Idprom Contents (hex)
(CPAK NVR1 Table - addr 0x8000-0x807F)
000: 01 21 09 03 00 00 00 00 1E AA
010: 4A 38 38 00 0A 00 0A 01 83 40
```

```
020: 86 60 00 00 00 04 40 50 26 17
030: 14 46 00 43 49 53 43 4F 20 20
040: 20 20 20 20 20 20 20 20 20 00
050: 00 0C 38 30 30 2D 34 31 34 39
060: 35 2D 30 31 20 20 20 20 46 42
070: 4E 31 38 31 37 32 30 38 33 31
080: 20 20 20 20 32 30 31 34 30 34
090: 32 34 00 00 57 4F 54 52 43 35
100: 50 42 41 41 6E 5A 00 05 02 03
110: 0C 03 0F 20 01 01 08 00 FE 01
120: 00 00 00 02 03 00 00 FC
Threshold Data (hex)
CPAK NVR2 Table - address 0x8080-0x80FF
000: 4B 00 46 00 00 00 FB 00 8A 00
010: 87 5A 7A 76 77 E2 00 00 00 00
020: 00 00 00 00 00 00 00 00 00 00
030: 00 00 00 00 00 00 00 00 00 00
040: 13 88 11 94 05 DC 03 E8 45 76
050: 22 D0 06 C9 03 66 5A 00 55 00
060: 00 00 FB 00 88 71 43 E2 04 62
070: 02 32 00 00 00 00 00 00 00 00
080: 00 00 00 00 00 00 00 00 00 00
090: 00 00 00 00 00 00 00 00 00 00
100: 00 00 00 00 00 00 00 00 00 00
110: 00 00 00 00 00 00 00 00 00 00
120: 00 00 00 00 00 00 00 93
Vendor Idprom Contents (hex)
Vendor Cisco NVR1 Table - address 0x8400-0x847F
000: 02 00 00 00 00 00 00 00 00 00
010: 00 00 00 00 00 00 43 49 53 43
020: 4F 20 20 20 20 20 20 20 20 20
030: 20 20 43 50 41 4B 2D 31 30 30
040: 47 2D 53 52 31 30 20 20 56 45
050: 53 31 07 46 42 4E 31 38 31 37
060: 32 30 38 33 38 30 30 2D 34 31
070: 34 39 35 2D 30 31 30 31 20 20
080: 00 00 00 00 00 00 00 00 00 00
090: 00 32 38 2D 31 31 30 32 30 2D
100: 30 34 00 00 00 00 00 00 00 00
110: 00 00 00 00 00 00 00 00 00 00
120: 00 00 00 00 00 00 00 1B
Vendor Idprom Contents 2 (hex)
Vendor CISCO NVR2 Table - address 0x8480-0x84FF
000: 00 00 00 00 00 00 00 00 00 00
010: 00 00 00 00 00 00 00 00 00 00
020: 00 00 00 00 00 00 00 00 00 00
030: 00 00 41 46 45 30 34 30 46 52
040: 20 20 20 20 20 20 20 20 41 46
050: 45 30 34 42 47 55 20 20 20 20
060: 20 20 20 20 00 00 00 00 00 00
070: 00 00 00 00 00 00 00 00 00 00
080: 53 52 31 34 34 30 31 30 37 39
090: 2D 30 36 20 20 20 00 00 00 00
100: 00 00 00 00 00 00 00 00 00 00
110: 00 00 00 00 00 00 00 00 00 00
120: 00 00 00 00 00 00 00 38
Module State Register: 0x0020
Module General Control Register: 0x0000
Global Alarm Status: 0x0000
Network Lanes Alarm and Warning Status: 0x0000
Network Lanes Fault Status Summary: 0x0000
Host Lanes Fault Status Summary: 0x0000
Module Fault and Warning, General Status Summary: 0x0002
Module Fault and Warning, Fault Status Summary: 0x0000
```

```
Fault and Warning status, Alarms and Warning 1: 0x0000
Multimode fiber supported length = 100 m
Enhanced options implemented:
Host Lane PRBS Supported
Enhanced options 2 implemented:
none
Diagnostic monitoring implemented:
Transmitted power measurement type
Received power measurement type
Diagnostic monitoring capability 1:
Transceiver temperature monitor
Transceiver power supply voltage monitor
Diagnostic monitoring capability 2:
Network Lane laser temperature monitor
Network Lane laser bias current monitor
Network Lane laser output power monitor
Network Lane received power monitor
```

show interfaces trunk

To display the interface-trunk information, use the **showinterfacestrunk** command in user EXEC or privileged EXEC mode.

show interfaces [*interface interface-number*] **trunk** [{**module** *number* | **vlan** *vlan*}]

Syntax Description

interface	(Optional) Interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **pos**, **atm**, and **ge-wan**.
interface-number	(Optional) Module and port number; see the "Usage Guidelines" section for valid values.
module *number*	(Optional) Specifies the module number; see the "Usage Guidelines" section for valid values.
vlan *vlan*	(Optional) Limits the display of switch port information to the specified VLAN. Range: 1 to 4094.

Command Default

This command has no default settings.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXI	This command was changed to add the optional **vlan***vlan* keyword and argument.

Usage Guidelines

The **pos**, **atm**, and **ge-wan** keywords are supported on systems that are configured with a Supervisor Engine 2.

If you do not specify a keyword, only information for trunking ports is displayed.

The *interface-number* designates the module and port number. Valid values depend on the chassis and module that are used. For example, if you have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the slot number are from 1 to 13 and valid values for the port number are from 1 to 48.

The **module***number* keyword and argument designate the module number and limit the display to interfaces on the module. Valid values depend on the chassis that is used. For example, if you have a 13-slot chassis, valid values for the module number are from 1 to 13.

Examples

This example shows how to display the interface-trunk information for module 5:

```
Router#
show interfaces trunk module 5
Port      Mode         Encapsulation  Status        Native vlan
```

```
Fa5/1     routed       negotiate      routed        1
Fa5/2     routed       negotiate      routed        1
Fa5/3     routed       negotiate      routed        1
Fa5/4     routed       negotiate      routed        1
Fa5/5     routed       negotiate      routed        1
Fa5/6     off          negotiate      not-trunking  10
Fa5/7     off          negotiate      not-trunking  10
Fa5/8     off          negotiate      not-trunking  1
Fa5/9     desirable    n-isl          trunking      1
Fa5/10    desirable    negotiate      not-trunking  1
Fa5/11    routed       negotiate      routed        1
Fa5/12    routed       negotiate      routed        1
.
.
.
Fa5/48    routed       negotiate      routed        1
Port      Vlans allowed on trunk
Fa5/1     none
Fa5/2     none
Fa5/3     none
Fa5/4     none
Fa5/5     none
Fa5/6     none
Fa5/7     none
Fa5/8     200
Fa5/9     1-1005
Fa5/10    none
Fa5/11    none
Fa5/12    none
.
.
.
Fa5/48    none
Port      Vlans allowed and active in management domain
Fa5/1     none
Fa5/2     none
Fa5/3     none
Fa5/4     none
Fa5/5     none
Fa5/6     none
Fa5/7     none
Fa5/8     200
Fa5/9     1-6,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-8
02,850,917,999,1002-1005
Fa5/10    none
Fa5/11    none
Fa5/12    none
.
.
.
Fa5/48    none
Port      Vlans in spanning tree forwarding state and not pruned
Fa5/1     none
Fa5/2     none
Fa5/3     none
Fa5/4     none
Fa5/5     none
Fa5/6     none
Fa5/7     none
Fa5/8     200
Fa5/9     1-6,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-8
02,850,917,999,1002-1005
Fa5/10    none
Fa5/11    none
```

```
.
.
.
Fa5/48    none
Router#
```

This example shows how to display the trunking information for active trunking ports:

```
Router#
show interfaces trunk
Port      Mode         Encapsulation  Status        Native vlan
Fa5/9     desirable    n-isl          trunking      1
Port      Vlans allowed on trunk
Fa5/9     1-1005
Port      Vlans allowed and active in management domain
Fa5/9     1-6,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-8
02,850,917,999,1002-1005
Port      Vlans in spanning tree forwarding state and not pruned
Fa5/9     1-6,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-8
02,850,917,999,1002-1005
Router#
```

This example shows how to limit the display information for interfaces on a specific VLAN:

```
Router> show interfaces trunk vlan 22
Router>
```

Related Commands

Command	Description
show interfaces	Displays the status and statistics for the interfaces in the chassis.

show interfaces tunnel

To display tunnel interface information, use the **showinterfacestunnel** command in privileged EXEC mode.

show interfaces tunnel *number* [**accounting**]

Syntax Description

number	Port line number.
accounting	(Optional) Displays the number of packets of each protocol type that have been sent through the interface.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	Support was added to display traffic information when the **tunnelroute-via** command is present in the configuration file.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.11S	This command was integrated into Cisco IOS XE Release 3.11S. The output was modified to display information about tunnel entropy calculation.

Examples

The following is sample output from the **showinterfacestunnel** command.

```
Device# show interfaces tunnel 4

Tunnel4 is up, line protocol is down
Hardware is Routing Tunnel
MTU 1500 bytes, BW 9 Kbit, DLY 500000 usec, rely 255/255, load 1/255
Encapsulation TUNNEL, loopback not set, keepalive set (10 sec)
Tunnel source 0.0.0.0, destination 0.0.0.0
Tunnel protocol/transport GRE/IP, key disabled, sequencing disabled
Tunnel Entropy Calculation Enabled (24-bit Key)
Last input never, output never, output hang never
Last clearing of “show interface” counters never
Output queue 0/0, 0 drops; input queue 0/75, 0 drops
Five minute input rate 0 bits/sec, 0 packets/sec
Five minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
```

```
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets, 0 restarts

Device# show interfaces tunnel 0 | include route-via

Tunnel route-via feature is on [Ethernet0, preferred]

Device# show interfaces tunnel 0 | include route-via

Tunnel route-via feature is on [Ethernet0, mandatory]
```

The table below describes significant fields shown in the display.

*Table 163: **show interfaces tunnel** Field Descriptions*

Field	Description
Tunnel is {up | down}	Interface is currently active and inserted into ring (up) or inactive and not inserted (down). On the Cisco 7500 series routers, gives the interface processor type, slot number, and port number.
line protocol is {up | down | administratively down}	Shows line protocol up if a valid route is available to the tunnel destination. Shows line protocol down if no route is available or if the route would be recursive.
Hardware	Specifies the hardware type.
MTU	Maximum transmission unit of the interface.
BW	Bandwidth of the interface, in kilobits per second.
DLY	Delay of the interface, in microseconds.
rely	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method is always TUNNEL for tunnels.
loopback	Indicates whether loopback is set or not.
keepalive	Indicates whether keepalives are set or not.
Tunnel source	IP address used as the source address for packets in the tunnel.
destination	IP address of the host destination.
Tunnel protocol	Tunnel transport protocol (the protocol that the tunnel is using). This is based on the **tunnelmode**command, which defaults to GRE.
key	ID key for the tunnel interface, unless disabled.
Tunnel Entropy Calculation	Achieves load balancing of tunnel packets in a network.

Field	Description
sequencing	Indicates whether the tunnel interface drops datagrams that arrive out of order. Can be disabled.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This counter is updated only when packets are process-switched, not when packets are fast-switched.
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by an interface. This counter is updated only when packets are process-switched, not when packets are fast-switched.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. *** indicates the elapsed time is too large to be displayed. 0:00:00 indicates that the counters were cleared more than 231 ms (and less than 232 ms) ago.
Output queue, drops Input queue, drops	Number of packets in output and input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped because of a full queue.
Five minute input rate, Five minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes. The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernet networks and bursts of noise on serial lines are often responsible for no input buffer events.
broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the minimum packet size of them medium.

Field	Description
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium.
CRC	Number of cyclic redundancy checksums generated by the originating LAN station or far-end device that do not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of a station transmitting bad data.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets.
overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be increased.
abort	Illegal sequence of one bits on a serial interface. This usually indicates a clocking problem between the serial interface and the data link equipment.
packets output	Total number of messages transmitted by the system.
bytes	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the far-end transmitter has been running faster than the near-end router's receiver can handle. This may never be reported on some interfaces.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors, because some datagrams may have more than one error, and others may have errors that do not fall into any of the specifically tabulated categories.
collisions	Number of messages retransmitted because of an Ethernet collision. Some collisions are normal. However, if your collision rate climbs to around 4 or 5 percent, you should consider verifying that there is no faulty equipment on the segment and/or moving some existing stations to a new segment. A packet that collides is counted only once in output packets.
interface resets	Number of times an interface has been reset. The interface may be reset by the administrator or automatically when an internal error occurs.
restarts	Number of times that the controller was restarted because of errors.
preferred	If the route is not available, forwards the traffic using any available route.

Field	Description
mandatory	Drops the traffic if the route is not available.

Related Commands

Command	Description
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show ip route	Displays the current state of the routing table.

show interfaces ucse

To display Cisco UCS E-Series Server interface statistics, use the **show interfaces ucse** command in privileged EXEC mode.

show interfaces ucse *slot/subslot/ucse-interface* [{**accounting** | **controller** | **counters** | **crb** | **dampening** | **description** | **etherchannel** | **history** | **irb** | **mac-accounting** | **monitor** | **mpls-exp** | **precedence** | **stats** | **summary** | **switchport**}]

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the NIM E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot number is 0.
ucse-interface	Number of the UCSE interface. **Note** For Cisco UCS E-Series Servers, the UCSE interface number can be 0 or 1.
accounting	(Optional) Displays the number of packets of each protocol type that have been sent through the interface.
controller	(Optional) Displays the interface, configuration, and controller status.
counters	(Optional) Displays the interface counters.
crb	(Optional) Displays interface routing or bridging information.
dampening	(Optional) Displays interface dampening information.
description	(Optional) Displays the interface description.
etherchannel	(Optional) Displays interface Ether Channel information.
history	(Optional) Displays interface history.
irb	(Optional) Displays interface routing or bridging information.
mac-accounting	(Optional) Displays interface MAC accounting information.
monitor	(Optional) Displays interface continuously.
mpls-exp	(Optional) Displays interface Multiprotocol Label Switching (MPLS) experimental accounting information.
precedence	(Optional) Displays interface precedence accounting information.
stats	(Optional) Displays the switching path, the packets in and packets out, and the characters in and characters out.

summary	(Optional) Displays the interface summary.
switchport	(Optional) Displays the switch port interface information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced on the Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Router (ISR).
Cisco IOS XE Release 3.15S	This command was supported on an additional platform: the NIM E-Series Network Compute Engine (NIM E-Series NCE) installed in a Cisco ISR 4000 Series.

Examples

The following example provides sample output from the **show interfaces ucse** *slot*/**0/0 switchport** command in an E-Series Server installed in a Cisco ISR 4000 series:

```
Router# show interfaces ucse 1/0/0 switchport

 Name: ucse 1/0/0
 Switchport: Enabled
 Administrative mode: trunk
 Operational Mode: trunk
 Administrative Trunking Encapsulation: dot1q
 Operational Trunking Encapsulation: native
 Negotiation of Trunking: Disabled
 Trunking Native Mode VLAN: 2352
 Trunking VLANs Enabled: 1-2349,2450-4094
 Voice VLAN: none
```

show interfaces unidirectional

To display the operational state of an interface with a receive-only transceiver, use the **showinterfacesunidirectional** command in user EXEC or privileged EXEC mode.

show interfaces [*interface interface-number*] **unidirectional** [**module** *number*]

Syntax Description

interface	(Optional) Interface type; possible valid values are **gigabitethernet** and **tengigabitethernet**
interface-number	(Optional) Module and port number; see the "Usage Guidelines" section for valid values.
module *number*	(Optional) Specifies the module number; see the "Usage Guidelines" section for valid values.

Command Default

This command has no default settings.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If you do not specify a keyword, only information for trunking ports is displayed.

The *interface-number* designates the module and port number. Valid values depend on the chassis and module that are used. For example, if you have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the slot number are from 2 to 13 and valid values for the port number are from 1 to 48.

The **module***number* keyword and argument designate the module number and limit the display to interfaces on the module. Valid values depend on the chassis that is used. For example, if you have a 13-slot chassis, valid values for the module number are from 2 to 13.

Examples

This example shows how to display the operational state of an interface with a receive-only transceiver:

```
Router# show interfaces gigabitethernet 5/2 unidirectional
Unidirectional configuration mode: send only
Unidirectional operational mode: receive only
CDP neighbour unidirectional configuration mode: off
Router#
```

Related Commands

Command	Description
show interfaces status	Displays the interface status or a list of interfaces in an error-disabled state on LAN ports only.
unidirectional	Configures the software-based UDE.

show interfaces vg-anylan

To display the information about the 100VG-AnyLAN port adapter on Cisco 7200 series routers and Cisco 7500 series routers, use the **showinterfacesvg-anylan** command in user EXEC or privileged EXEC mode.

Cisco 7200 Series
show interfaces vg-anylan [*slot*/*port*]

Cisco 7500 Series with VIPs
show interfaces vg-anylan [*slot*/*port-adapter*/*port*]

Syntax Description

slot	(Optional) Slot number. Refer to the appropriate hardware manual for slot and port information.
port	(Optional) Port number. Refer to the appropriate hardware manual for slot and port information.
port-adapter	(Optional) Port adapter number. Refer to the appropriate hardware manual for information about port adapter compatibility.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **showinterfacesvg-anylan** command:

```
Router# show interfaces vg-anylan 3/0/0
VG-AnyLAN3/0/0 is up, line protocol is up
  Hardware is cyBus VG-AnyLAN Interface
  Frame type is 802.3, address is 0060.3e64.2460 (bia 0060.3e64.2460)
  Internet address is 10.1.1.5/16
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:26, output 00:00:09, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     5316 packets input, 857349 bytes, 0 no buffer
     Received 5310 broadcasts, 0 runts, 0 giants
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     7920 packets output, 754259 bytes, 0 underruns
```

```
0 output errors, 0 collisions, 2 interface resets
0 output buffer failures, 0 output buffers swapped out
0 vg alignment error, 0 vg balance error
0 vg invalid ipm error, 0 vg symbol error
0 vg skew error, 0 vg frame delimit error
0 vg high priority packets, 0 vg high priority octets
0 output errors, 0 collisions, 2 interface resets
0 output buffer failures, 0 output buffers swapped out
0 vg alignment error, 0 vg balance error
0 vg invalid ipm error, 0 vg symbol error
0 vg skew error, 0 vg frame delimit error
0 vg high priority packets, 0 vg high priority octets
```

The table below describes significant fields shown in the display.

*Table 164: **show interfaces vg-anylan** Field Descriptions*

Field	Description
VG-AnyLAN3/0/0 is up, line protocol is up	Indicates if the interface hardware is currently active and can transmit and receive or if it has been taken down by an administrator.
Hardware is cyBus VG-AnyLAN	Hardware type.
Frame type is 803.2	Currently the frame type supported is 803.2.
Internet address	Internet address and subnet mask.
MTU	Maximum transmission unit of the interface.
BW	Bandwidth of the interface, in kilobits per second.
DLY	Delay of the interface, in microseconds.
rely	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes. The calculation uses the value from the **bandwidth** interface configuration command.
Encapsulation	Encapsulation method assigned to the interface.
loopback	Indicates if loopbacks are set.
keepalive	Indicates if keepalives are set.
ARA type	ARP type on the interface.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This counter is updated only when packets are process-switched, not when packets are fast-switched.

Field	Description
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by an interface. This counter is updated only when packets are process-switched, not when packets are fast-switched.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.
last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. *** indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 231 ms (and less than 232 ms) ago.
Queueing strategy	First-in, first-out queueing strategy (other queueing strategies that you might see are priority-list, custom-list, and weighted fair).
Output queue, drops input queue, drops	Number of packets in output and input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped because a queue was full.
5 minute input rate 5 minute output rate	Average number of bits and packets received or transmitted per second in the last 5 minutes.
packets input	Total number of error-free packets received by the system.
bytes (input)	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernet networks and bursts of noise on serial lines are often responsible for no input buffer events.
broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium.
input errors	Total number of no buffer, runts, giants, CRCs, frame, overrun, ignored, and abort counts. Other input-related errors can also increment the count, so that this sum might not balance with the other counts.

Field	Description
CRC	Cyclic redundancy checksum generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data. On a serial link, CRCs usually indicate noise, gain hits or other transmission problems on the data link.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a serial line, this is usually the result of noise or other transmission problems.
overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be incremented.
abort	Illegal sequence of one bits on the interface.
input packets with dribble condition detected	Dribble bit error indicates that a frame is slightly too long. This frame error counter is incremented just for informational purposes; the router accepts the frame.
packets output	Total number of messages transmitted by the system.
bytes (output)	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the far-end transmitter has been running faster than the near-end router's receiver can handle.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this might not balance with the sum of the enumerated output errors, as some datagrams can have more than one error, and others can have errors that do not fall into any of the specifically tabulated categories.
collisions	Number of messages retransmitted because of an Ethernet collision. A packet that collides is counted only once in output packets.
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within a certain interval. If the system notices that the carrier detect line of an interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an unrecoverable interface processor error occurred, or when an interface is looped back or shut down.
output buffer failures	Number of times that a packet was not output from the output hold queue because of a shortage of MEMD shared memory.

Field	Description
output buffers swapped out	Number of packets stored in main memory when the output queue is full; swapping buffers to main memory prevents packets from being dropped when output is congested. The number is high when traffic is bursty.
vg alignment error	Number of nonoctets received.
vg balance error	Number of incorrect balanced symbols received.
vg invalid ipm error	Number of packets received with an invalid packet marker (IPM).
vg symbol error	Number of symbols received that were not correctly decoded.
vg skew error	Number of skews between four pairs of twisted-pair wire that exceeded the allowable skew.
vg frame delimit error	Number of start-of-frame errors or false-start errors received.
vg high priority packets	Number of high-priority packets received.
vg high priority octets	Number of high-priority octets received.

Related Commands

Command	Description
interface vg-anylan	Specifies the interface on a 100VG-AnyLAN port adapter and enters interface configuration mode on Cisco 7200 series routers and Cisco 7500 series routers.

show interfaces vlan mapping through show scp

show interface gigabitethernet

To display the first front panel interface (port 0) in a Cisco 4451 ISR, use the **showinterfaces gigabitethernet** command in privileged EXEC mode.

show interfaces gigabitethernet {**ports**}

Syntax Description

interface gigabitethernet	Displays interface hardware.
ports	Displays local and registered IPC ports.

Command Modes

Privileged EXEC

Command History

Release	Modification
XE 16.11.1	This command was introduced.

Usage Guidelines

You can use the **show interfaces gigabitethernet** command to display the first front panel interface (port 0) in a Cisco ISR4451-X router

Examples

The following is sample output from the showcommand with the **ports**keyword displays he first front panel interface (port 0) in a Cisco ISR4451-X router::

```
Router# show interfaces gigabitethernet GigabitEthernet0/0/0 is down, line protocol is down

  Hardware is ISR4451-X-4x1GE, address is 003a.7d5e.8b40 (bia 003a.7d5e.8b40)
  Internet address is 10.20.30.40/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full Duplex, 1000Mbps, link type is auto, media type is SX
  output flow-control is off, input flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 02:45:34, output 02:00:47, output hang never
  Last clearing of "show interface" counters 1d16h
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
     618 packets input, 52156 bytes, 0 no buffer
     Received 447 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 145 multicast, 118 pause input
     189 packets output, 18556 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     597 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

The table below describes the significant fields shown in the display.

Table 165: show interfaces gigabitethernet Field Descriptions-Front Panel Gigabit Ethernet Port

Field	Description
GigabitEthernet0/0/0 is down, line protocol is down	Indicates whether the interface hardware is currently active and if it has been taken down by an administrator..
line protocol is	Indicates whether the software processes that handle the line protocol consider the line usable or if it has been taken down by an administrator.
Hardware	Hardware type and MAC address.
Description	Alphanumeric string identifying the interface. This appears only if the description interface configuration command has been configured on the interface.
Internet address	Sequence number of the in-sequence message that was last heard.
MTU	Maximum transmission unit of the interface.
BW	Bandwidth of the interface in kilobits per second.
DLY	Delay of the interface in microseconds.
Reliability	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes
Rxload and Rxload	Load on the interface (in the transmit “tx” and receive “rx” directions) as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method assigned to the interface.
Loopback	Indicates whether loopback is set.
Keepalive	Indicates whether keepalives are set, and the time interval.
Half-duplex, Full-duplex	Indicates the duplex mode for the interface.
1Gb/s	Speed of the interface in Gigabits per second.
Input Flow Rate…	Specifies if input flow control is on or off.
ARP Type	Type of ARP assigned and the timeout period.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the router. Useful for knowing when a dead interface failed. This field is not updated by fast-switched traffic
Output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by the interface. Useful for knowing when a dead interface failed.

Field	Description
Output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is displayed. If that field overflows, asterisks are printed
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. A series of asterisks (***) indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 231 ms (and less than 232 ms) ago.
Input queue (size/max/drops/flushes)	Packet statistics on the input queue reported as: • Size--Number of packets in the input queue. • Max--Maximum size of the queue. • Drops--Number of packets dropped because of a full input queue. • Flushes--Number of packets dropped as part of SPD. SPD implements a selective packet drop
Total Output Drops	Total number of packets dropped because of a full output queue.
Queueing Strategy	Type of Layer 3 queueing active on this interface. The default is FIFO.
Output queue (size/max)	Number of packets in the output queue (size), and the maximum size of the queue (max).
30 second input rate, 30 second output rate	Average number of bits and packets transmitted per second in the last 30 seconds. If the interface is not in promiscuous mode, it senses network traffic it sends and receives (rather than all network traffic). The 30 second input and output rates should be used only as an approximation of traffic per second during a given 30 second period. These rates are exponentially weighted averages with a time constant of 30 seconds. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period. The calculated input rate includes packets counted as input errors.
Packets Input	Total number of packets received by the system.
Bytes	Total number of bytes, including data and MAC encapsulation, in all packets received by the system.
Received…Broadcasts	Total number of broadcast or multicast packets received by the interface.
Runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium.
giants	

Field	Description
Throttles	Number of times the receiver on the port was disabled, possibly because of buffer or processor overload.
Input errors	Includes runts, giants, no buffer, CRC, frame, overrun, and ignored counts. Other input-related errors can also cause the input errors count to be increased, and some datagrams may have more than one error; therefore, this sum may not balance with the sum of enumerated input error counts.
CRC	Cyclic redundancy check generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data.
Frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a LAN, this is usually the result of collisions or a malfunctioning Ethernet device.
Overrun	Number of times the receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
Ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers. Broadcast storms and bursts of noise can cause the ignored count to be increased.
Watchdog	Number of times the watchdog receive timer expired.
Multicast	Number of multicast packets.
Pause input	Number of pause packets received.
Packets output	Total number of messages transmitted by the system.
Bytes	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
Underruns	Number of times that the transmitter has been running faster than the router can handle.
Output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors, because some datagrams may have more than one error and others may have errors that do not fall into any of the specifically tabulated categories.
Collisions	Number of messages retransmitted because of an Ethernet collision. This is usually the result of an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). A packet that collides is counted only once in output packets.

Field	Description
Interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within several seconds. Interface resets can occur when an interface is looped back or shut down.
Babbles	Transmit jabber timer expired.
Late collision	Number of late collisions. Late collision happens when a collision occurs after transmitting the preamble.
Deferred	Number of times that the interface had to defer while ready to transmit a frame because the carrier was asserted.
Lost carrier	Number of times the carrier was lost during transmission.
No carrier	Number of times the carrier was not present during the transmission.
Pause output	Number of pause packets transmitted.
Output buffer failures, Output buffers swapped out	Number of output butters failures and output buffers swapped out.

Related Commands

Command	Description
show ip interface	Display the usability status of interfaces configured for IP,.

show interfaces vlan mapping

To display the status of a virtual local area network (VLAN) mapping on a port, use the **showinterfacesvlanmapping** command in user EXEC or privileged EXEC mode.

show interfaces *interface interface-number* **vlan mapping**

Syntax Description

interface	Interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **pos**, **atm**, and **ge-wan**.
interface-number	Module and port number; see the “Usage Guidelines” section for valid values.

Command Default

This command has no default settings.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(17b)SXA	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **pos**, **atm**, and **ge-wan** keywords are supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

The *interface-number* designates the module and port number. Valid values depend on the chassis and module that are used. For example, if you have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the slot number are from 1 to 13 and valid values for the port number are from 1 to 48.

Examples

This example shows how to list all of the VLAN mappings that are configured on a port and indicate whether such mappings are enabled or disabled on the port:

```
Router# show interfaces gigabitethernet 5/2 vlan mapping
State: enabled
Original VLAN Translated VLAN
------------- ---------------
  1649           755
Router#
```

Related Commands

Command	Description
show vlan mapping	Registers a mapping of an 802.1Q VLAN to an ISL VLAN.
switchport vlan mapping enable	Enables VLAN mapping per switch port.

show interfaces wlan-controller

To show the Cisco Wireless Local Area Network (WLAN) controller network module interfaces on the router, use the **showinterfaceswlan-controller** command in privileged EXEC mode.

show interfaces wlan-controller slot/unit

Syntax Description

slot/unit	Specifies the router slot and unit numbers for the WLAN controller network module.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(2)XA1	This command was introduced on the router software.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.

Examples

The following example shows how to read the hardware information about the interface WLAN controller in the router:

```
Router# show interfaces wlan-controller 1/0
wlan-controller1/0 is up, line protocol is up
  Hardware is I82559FE, address is 0005.9a3d.7450 (bia 0005.9a3d.7450)
  Internet address is 30.0.0.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID  1., loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:05, output 00:00:03, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     2400779 packets input, 143127299 bytes
     Received 2349587 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     468232 packets output, 106333102 bytes, 0 underruns
     0 output errors, 0 collisions, 3 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 1 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

show ip interface

To display the usability status of interfaces configured for IP, use the **show ip interface** command in privileged EXEC mode.

show **ip** **interface** [*type* *number*] [**brief**]

Syntax Description

type	(Optional) Interface type.
number	(Optional) Interface number.
brief	(Optional) Displays a summary of the usability status information for each interface.

Command Default

The full usability status is displayed for all interfaces configured for IP.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.0(3)T	The command output was modified to show the status of the **ip wccp redirect out** and **ip wccp redirect exclude add in** commands.
12.2(14)S	The command output was modified to display the status of NetFlow on a subinterface.
12.2(15)T	The command output was modified to display the status of NetFlow on a subinterface.
12.3(6)	The command output was modified to identify the downstream VPN routing and forwarding (VRF) instance in the output.
12.3(14)YM2	The command output was modified to show the usability status of interfaces configured for Multiprocessor Forwarding (MPF) and implemented on the Cisco 7301 and Cisco 7206VXR routers.
12.2(14)SX	This command was implemented on the Supervisor Engine 720.
12.2(17d)SXB	This command was integrated into Cisco IOS 12.2(17d)SXB on the Supervisor Engine 2, and the command output was changed to include NDE for hardware flow status.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	The command output was modified to display information about the Unicast Reverse Path Forwarding (RPF) notification feature.

Release	Modification
12.4(20)T	The command output was modified to display information about the Unicast RPF notification feature.
12.2(33)SXI2	This command was modified. The command output was modified to display information about the Unicast RPF notification feature.
Cisco IOS XE Release 2.5	This command was modified. This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.9S	This command was implemented on Cisco 4400 Series ISRs.

Usage Guidelines

The Cisco IOS software automatically enters a directly connected route in the routing table if the interface is usable (which means that it can send and receive packets). If an interface is not usable, the directly connected routing entry is removed from the routing table. Removing the entry lets the software use dynamic routing protocols to determine backup routes to the network, if any.

If the interface can provide two-way communication, the line protocol is marked "up." If the interface hardware is usable, the interface is marked "up."

If you specify an optional interface type, information for that specific interface is displayed. If you specify no optional arguments, information on all the interfaces is displayed.

When an asynchronous interface is encapsulated with PPP or Serial Line Internet Protocol (SLIP), IP fast switching is enabled. A **show ip interface** command on an asynchronous interface encapsulated with PPP or SLIP displays a message indicating that IP fast switching is enabled.

You can use the **show ip interface brief** command to display a summary of the router interfaces. This command displays the IP address, the interface status, and other information.

The **show ip interface brief** command does not display any information related to Unicast RPF.

Examples

The following example shows configuration information for interface Gigabit Ethernet 0/3. In this example, the IP flow egress feature is configured on the output side (where packets go out of the interface), and the policy route map named PBRNAME is configured on the input side (where packets come into the interface).

```
Router# show running-config interface gigabitethernet 0/3
interface GigabitEthernet0/3
 ip address 10.1.1.1 255.255.0.0
 ip flow egress
 ip policy route-map PBRNAME
 duplex auto
 speed auto
 media-type gbic
 negotiation auto
end
```

The following example shows interface information on Gigabit Ethernet interface 0/3. In this example, MPF is enabled, and both Policy Based Routing (PBR) and NetFlow features are not supported by MPF and are ignored.

```
Router# show ip interface gigabitethernet 0/3
```

```
GigabitEthernet0/3 is up, line protocol is up
  Internet address is 10.1.1.1/16
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP Feature Fast switching turbo vector
  IP VPN Flow CEF switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is enabled, using route map PBR
  Network address translation is disabled
  BGP Policy Mapping is disabled
  IP Multi-Processor Forwarding is enabled
     IP Input features, "PBR",
         are not supported by MPF and are IGNORED
     IP Output features, "NetFlow",
         are not supported by MPF and are IGNORED
```

The following example identifies a downstream VRF instance. In the example, "Downstream VPN Routing/Forwarding "D"" identifies the downstream VRF instance.

```
Router# show ip interface virtual-access 3
Virtual-Access3 is up, line protocol is up
  Interface is unnumbered. Using address of Loopback2 (10.0.0.8)
  Broadcast address is 255.255.255.255
  Peer address is 10.8.1.1
  MTU is 1492 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is enabled
  IP Flow switching is disabled
  IP CEF switching is enabled
```

```
  IP Feature Fast switching turbo vector
  IP VPN CEF switching turbo vector
  VPN Routing/Forwarding "U"
  Downstream VPN Routing/Forwarding "D"
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
```

The following example shows the information displayed when Unicast RPF drop-rate notification is configured:

```
Router# show ip interface ethernet 2/3
Ethernet2/3 is up, line protocol is up
  Internet address is 10.0.0.4/16
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP Flow switching is disabled
  IP CEF switching is disabled
  IP Null turbo vector
  IP Null turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are No CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
```

Unicast RPF Information

```
  Input features: uRPF
  IP verify source reachable-via RX, allow default
   0 verification drops
   0 suppressed verification drops
   0 verification drop-rate
Router#
```

The following example shows how to display the usability status for a specific VLAN:

```
Router# show ip interface vlan 1
Vlan1 is up, line protocol is up
  Internet address is 10.0.0.4/24
  Broadcast address is 255.255.255.255
Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP Fast switching turbo vector
  IP Normal CEF switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
  Sampled Netflow is disabled
  IP multicast multilayer switching is disabled
  Netflow Data Export (hardware) is enabled
```

The table below describes the significant fields shown in the display.

Table 166: show ip interface Field Descriptions

Field	Description
Virtual-Access3 is up	Shows whether the interface hardware is usable (up). For an interface to be usable, both the interface hardware and line protocol must be up.
Broadcast address is	Broadcast address.
Peer address is	Peer address.
MTU is	MTU value set on the interface, in bytes.
Helper address	Helper address, if one is set.
Directed broadcast forwarding	Shows whether directed broadcast forwarding is enabled.
Outgoing access list	Shows whether the interface has an outgoing access list set.
Inbound access list	Shows whether the interface has an incoming access list set.
Proxy ARP	Shows whether Proxy Address Resolution Protocol (ARP) is enabled for the interface.
Security level	IP Security Option (IPSO) security level set for this interface.
Split horizon	Shows whether split horizon is enabled.
ICMP redirects	Shows whether redirect messages will be sent on this interface.
ICMP unreachables	Shows whether unreachable messages will be sent on this interface.
ICMP mask replies	Shows whether mask replies will be sent on this interface.
IP fast switching	Shows whether fast switching is enabled for this interface. It is generally enabled on serial interfaces, such as this one.
IP Flow switching	Shows whether Flow switching is enabled for this interface.
IP CEF switching	Shows whether Cisco Express Forwarding switching is enabled for the interface.
Downstream VPN Routing/Forwarding "D"	Shows the VRF instance where the PPP peer routes and AAA per-user routes are being installed.
IP multicast fast switching	Shows whether multicast fast switching is enabled for the interface.
IP route-cache flags are Fast	Shows whether NetFlow is enabled on an interface. Displays "Flow init" to specify that NetFlow is enabled on the interface. Displays "Ingress Flow" to specify that NetFlow is enabled on a subinterface using the **ip flow ingress**command. Shows "Flow" to specify that NetFlow is enabled on a main interface using the **ip route-cache flow** command.

Field	Description
Router Discovery	Shows whether the discovery process is enabled for this interface. It is generally disabled on serial interfaces.
IP output packet accounting	Shows whether IP accounting is enabled for this interface and what the threshold (maximum number of entries) is.
TCP/IP header compression	Shows whether compression is enabled.
WCCP Redirect outbound is disabled	Shows the status of whether packets received on an interface are redirected to a cache engine. Displays "enabled" or "disabled."
WCCP Redirect exclude is disabled	Shows the status of whether packets targeted for an interface will be excluded from being redirected to a cache engine. Displays "enabled" or "disabled."
Netflow Data Export (hardware) is enabled	NetFlow Data Expert (NDE) hardware flow status on the interface.

The table below describes the significant fields shown in the display.

Display a Summary of Interfaces on Cisco 4400 Series ISR: Example

The following is a sample out of the **show ip interface brief** command displaying a summary of the interfaces and their status on the device.

```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/1   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/2   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/3   unassigned      YES NVRAM  down                  down
Serial1/0/0            unassigned      YES unset  down                  down
GigabitEthernet0       unassigned      YES NVRAM  up                    up
```

Display a Summary of the Usability Status: Example

The following example shows how to display a summary of the usability status information for each interface:

```
Router# show ip interface brief
Interface     IP-Address     OK?  Method  Status                  Protocol
Ethernet0     10.108.00.5    YES  NVRAM   up                      up
Ethernet1     unassigned     YES  unset   administratively down   down
Loopback0     10.108.200.5   YES  NVRAM   up                      up
Serial0       10.108.100.5   YES  NVRAM   up                      up
Serial1       10.108.40.5    YES  NVRAM   up                      up
Serial2       10.108.100.5   YES  manual  up                      up
Serial3       unassigned     YES  unset   administratively down   down
```

Table 167: show ip interface brief Field Descriptions

Field	Description
Interface	Type of interface.
IP-Address	IP address assigned to the interface.
OK?	"Yes" means that the IP Address is valid. "No" means that the IP Address is not valid.
Method	The Method field has the following possible values: • RARP or SLARP--Reverse Address Resolution Protocol (RARP) or Serial Line Address Resolution Protocol (SLARP) request. • BOOTP--Bootstrap protocol. • TFTP--Configuration file obtained from the TFTP server. • manual--Manually changed by the command-line interface. • NVRAM--Configuration file in NVRAM. • IPCP--**ip address negotiated** command. • DHCP--**ip address dhcp** command. • unset--Unset. • other--Unknown.
Status	Shows the status of the interface. Valid values and their meanings are: • up--Interface is up. • down--Interface is down. • administratively down--Interface is administratively down.
Protocol	Shows the operational status of the routing protocol on this interface.

Related Commands

Command	Description
ip address	Sets a primary or secondary IP address for an interface.
ip vrf autoclassify	Enables VRF autoclassify on a source interface.
match ip source	Specifies a source IP address to match to required route maps that have been set up based on VRF connected routes.
route-map	Defines the conditions for redistributing routes from one routing protocol into another or to enable policy routing.
set vrf	Enables VPN VRF selection within a route map for policy-based routing VRF selection.

Command	Description
show ip arp	Displays the ARP cache, in which SLIP addresses appear as permanent ARP table entries.
show route-map	Displays static and dynamic route maps.

show ipc

To display interprocess communication (IPC) statistics, use the **showipc** command in privileged EXEC mode.

show ipc {**nodes** | **ports** [**open**] | **queue** | **status** [**cumulative**] | **zones**}

Syntax Description

nodes	Displays participating nodes.
ports	Displays local and registered IPC ports.
open	(Optional) Displays local IPC ports that have been opened by the current seat (node).
queue	Displays information about the IPC retransmission queue and the IPC message queue.
status	Displays the status of the local IPC server.
cumulative	(Optional) Displays cumulative totals for the status counters of the local IPC server since the router was rebooted.
zones	Displays information about the IPC zones and seats.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(12c)EW	This command was introduced.
12.2(15)T	The **cumulative** keyword was added.
12.3(7)T	The **zones** keyword was added.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to 12.2(17d)SXB.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The Cisco IOS version of IPC provides a reliable ordered delivery of messages using an underlying platform driver transport or User Datagram Protocol (UDP) transport protocol.

Nodes

A node (referred to as a seat) is an intelligent element like a processor that can communicate using IPC services. A seat is where entities and ports reside. A seat manager performs all the interprocessor communications by receiving messages from the network and forwarding the messages to the appropriate port.

Ports

IPC communication endpoints (ports) receive and queue received IPC messages.

Queue

Use the **queue** keyword to display information about the IPC retransmission queue and the IPC message queue.

Status

Use the**status** keyword to display the IPC statistics that have been generated since a **clearipcstatistics** command was entered. The **showipcstatus** command with the **cumulative** keyword displays the IPC statistics that have been gathered since the router was rebooted, regardless of how many times the statistics have been cleared.

Zones

The IPC zone manager allows more than one group of IPC seats to exist to enable direct communication between line cards and the route processor. Use the**zones** keyword to display the IPC zone and seat information.

Examples

The following is sample output from the **showipc**command with the **nodes**keyword displaying the participating seats (nodes):

```
Router# show ipc nodes
There are 6 nodes in this IPC realm.
   ID      Type       Name                      Last  Last
                                                Sent Heard
0.10000    Local      IPC Master                  0     0
0.1060000  RSP-CY     RSP IPC card slot 6         9    79
0.1050000  RSP-CY     RSP IPC card slot 5        21    22
0.1080000  RSP-CY     RSP IPC card slot 8        21    22
1.10000    Local      IPC Master: -Zone#1         0     0
2.10000    Local      IPC Master: -Zone#2
```

The table below describes the significant fields shown in the display.

Table 168: show ipc nodes Field Descriptions

Field	Description
ID	Port ID, which consists of a zone ID followed by the seat ID.
Type	Type of seat (node).
Name	Seat name.
Last Sent	Sequence number of the message that was last sent.
Last Heard	Sequence number of the in-sequence message that was last heard.

The following is sample output from the **showipc**command with the **ports**keyword displaying the local and registered IPC ports:

```
Router# show ipc ports
There are 11 ports defined.

Port ID     Type    Name            (current/peak/total)
1.10000.1   unicast IPC Master:Zone
1.10000.2   unicast IPC Master:Echo
1.10000.3   unicast IPC Master:Control
1.10000.4   unicast Remote TTY Server Port
1.10000.5   unicast GALIOS RF :Active
index = 0 seat_id = 0x2020000 last sent = 0 heard = 1635 0/1/1635
1.10000.6   unicast GALIOS RED:Active
```

```
index = 0 seat_id = 0x2020000 last sent = 0 heard = 2 0/1/2

2.2020000.3 unicast GALIOS IPC:Card 2:Control
2.2020000.4 unicast GALIOS RFS :Standby
2.2020000.5 unicast Slave: Remote TTY Client Port
2.2020000.6 unicast GALIOS RF :Standby
2.2020000.7 unicast GALIOS RED:Standby
RPC packets: current/peak/total 0/1/17
```

The table below describes the significant fields shown in the display.

Table 169: show ipc ports Field Descriptions

Field	Description
Port ID	Port ID, which consists of a zone ID followed by the seat ID.
Type	Type of port.
Name	Port name.
current/peak/total	Displays information about the number of messages held by this IPC session.

The following is sample output from the **showipc**command with the **queue**keyword displaying information about the IPC retransmission queue and the IPC message queue:

```
Router# show ipc queue
There are 0 IPC messages waiting for acknowledgement in the transmit queue.
There are 0 IPC messages waiting for a response.
There are 0 IPC messages waiting for additional fragments.
There are 0 IPC messages currently on the IPC inboundQ.
There are 0 messages currently in use by the system.
```

The following is sample output from the **showipc**command with the **status**keyword displaying information about the local IPC server:

```
Router# show ipc status
IPC System Status
Time last IPC stat cleared : never
This processor is the IPC master server.
Do not drop output of IPC frames for test purposes.
1000 IPC Message Headers Cached.
                                                      Rx Side     Tx Side
Total Frames                                              189         140
Total from Local Ports                                    189          70
Total Protocol Control Frames                              70          44
Total Frames Dropped                                        0           0
                           Service Usage
Total via Unreliable Connection-Less Service              145           0
Total via Unreliable Sequenced Connection-Less Svc          0           0
Total via Reliable Connection-Oriented Service             44          70
                            IPC Protocol Version 0
Total Acknowledgements                                     70          44
Total Negative Acknowledgements                             0           0
                            Device Drivers
Total via Local Driver                                      0           0
Total via Platform Driver                                   0          70
Total Frames Dropped by Platform Drivers                    0           0
                    Reliable Tx Statistics
Re-Transmission                                                         0
```

```
Re-Tx Timeout                                                        0
Rx Errors                          Tx Errors
Unsupp IPC Proto Version         0  Tx Session Error              0
Corrupt Frame                    0  Tx Seat Error                 0
Duplicate Frame                  0  Destination Unreachable       0
Out-of-Sequence Frame            0  Tx Test Drop                  0
Dest Port does Not Exist         0  Tx Driver Failed              0
Rx IPC Msg Alloc Failed          0  Ctrl Frm Alloc Failed         0
Unable to Deliver Msg            0
         Buffer Errors                       Misc Errors
IPC Msg Alloc                    0  IPC Open Port                 0
Emer IPC Msg Alloc               0  No HWQ                        0
IPC Frame PakType Alloc          0  Hardware Error                0
IPC Frame MemD Alloc             0
         Tx Driver Errors
No Transport                     0
MTU Failure                      0
Dest does not Exist              0
```

The table below describes the significant fields shown in the display.

Table 170: show ipc status Field Descriptions

Field	Description
Time last IPC stat cleared	Displays the time, in dd:hh:mm (or never), since the IPC statistics were last cleared.
This processor is	Shows whether the processor is the IPC master or an IPC slave.
IPC Message Headers Cached	Number of message headers available in the IPC message cache.
Rx Side	Information about IPC messages received.
Tx Side	Information about IPC messages sent.
Service Usage	Number of IPC messages received or sent via connectionless or connection-oriented protocols.
IPC Protocol Version 0	Number of acknowledgements and negative acknowledgements received or sent by the system.
Device Drivers	Number of IPC messages received or sent using the underlying device drivers.
Reliable Tx Statistics	Number of IPC messages that were retransmitted or that timed out on retransmission using a reliable connection-oriented protocol.
Rx Errors	Number of IPC messages received that displayed various internal frame or delivery errors.
Tx Errors	Number of IPC messages sent that displayed various transmission errors.
Buffer Errors	Number of message allocation failures from the IPC message cache, IPC emergency message cache, IPC frame allocation cache, and IPC frame memory allocation cache.
Misc Errors	Various miscellaneous errors that relate to the IPC open queue, to the hardware queue, or to other hardware failures.

Field	Description
Tx Driver Errors	Number of messages that relate to IPC transmission driver failures including messages to or from a destination without a valid transport entity from the seat; number of messages dropped because the packet size is larger than the maximum transmission unit (MTU); and number of messages without a valid destination address.

The following example shows how to display cumulative IPC counters for the local IPC server. Note that the recent IPC clearing has not cleared the IPC counters because the **cumulative** keyword displays the IPC statistics that have been generated since the router was rebooted.

```
Router# show ipc status cumulative
IPC System Status
Time last IPC stat cleared : 00:00:05
This processor is the IPC master server.
Do not drop output of IPC frames for test purposes.
1000 IPC Message Headers Cached.
                                                      Rx Side     Tx Side
Total Frames                                             3473         184
Total from Local Ports                                   3473          92
Total Protocol Control Frames                              92          54
Total Frames Dropped                                        0           0
                             Service Usage
Total via Unreliable Connection-Less Service             2449           0
Total via Unreliable Sequenced Connection-Less Svc        970           0
Total via Reliable Connection-Oriented Service             54          92
                     IPC Protocol Version 0
Total Acknowledgements                                      0           0
Total Negative Acknowledgements                             0           0
                            Device Drivers
Total via Local Driver                                      0           0
Total via Platform Driver                                   0          92
Total Frames Dropped by Platform Drivers                    0           0
                    Reliable Tx Statistics
Re-Transmission                                                         0
Re-Tx Timeout                                                           0
Rx Errors                               Tx Errors
Unsupp IPC Proto Version          0  Tx Session Error                  0
Corrupt Frame                     0  Tx Seat Error                     0
Duplicate Frame                   0  Destination Unreachable           0
Out-of-Sequence Frame             0  Tx Test Drop                      0
Dest Port does Not Exist          0  Tx Driver Failed                  0
Rx IPC Msg Alloc Failed           0  Ctrl Frm Alloc Failed             0
Unable to Deliver Msg             0
         Buffer Errors                        Misc Errors
IPC Msg Alloc                     0  IPC Open Port                     0
Emer IPC Msg Alloc                0  No HWQ                            0
IPC Frame PakType Alloc           0  Hardware Error                    0
IPC Frame MemD Alloc              0
         Tx Driver Errors
No Transport                      0
MTU Failure                       0
Dest does not Exist               0
```

The following is sample output from the **showipc**command with the **zones**keyword displaying information about the IPC zones and seats:

```
Router# show ipc zones
There are 3 Zones in this IPC realm.
```

```
Zone ID   Seat ID   Name
      0    10000    IPC Default Zone
      1    10000    IPC TEST ZONE#1
      2    10000    IPC TEST ZONE#2
```

The table below describes the significant fields shown in the display.

Table 171: show ipc zones Field Descriptions

Field	Description
Zone ID	Zone number.
Seat ID	Seat number.
Name	Zone name.

Related Commands

Command	Description
clear ipc statistics	Clears and resets the IPC statistics.

show ipc hog-info

To provide information about interprocess communication (IPC) messages that consume excessive CPU, use the **showipchog-info**command in privileged EXEC mode.

show ipc hog-info

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The Cisco IOS version of IPC provides a reliable ordered delivery of messages using an underlying platform driver transport or User Datagram Protocol (UDP) transport protocol.

The show ipc hog-info command displays information about IPC messages that are being processed when a CPUHOG error occurs, indicating that the client processing an IPC message is using too much CPU, or when an IPC message callback exceeds 200 milliseconds.

Examples

The following example shows that the IPC process has had a CPUHOG error or the message callback exceeded the 200-millisecond threshold:

```
Router# show ipc hog-info
Time last IPC process hogged CPU: 00:05:09
IPC Messages Processed:
Source       Destination  Name                         Message-Type  Time-taken
                                                           (0x)       (msec)
 1030000     10000.14    ISSU Process: Active Por         0         864
 1030000     10000.D     RF : Active                      0           0
```

In the following example, the show ipc status command shows a counter incrementing whenever a callback exceeds 200 milliseconds:

```
Router# show ipc status
                            IPC System Status
 Time last IPC stat cleared : never
 This processor is the IPC master server.
 Do not drop output of IPC frames for test purposes.
 1000 IPC Message Headers Cached.
                                                    Rx Side     Tx Side
 Total Frames                                          9501        3973
 Total from Local Ports                               14328        3258
 Total Protocol Control Frames                         1628         713
 Total Frames Dropped                                     0           0
                             Service Usage
 Total via Unreliable Connection-Less Service          7865           0
```

```
Total via Unreliable Sequenced Connection-Less Svc         0           0
Total via Reliable Connection-Oriented Service           831        1629
                     IPC Protocol Version 0


Total Acknowledgments                                  1628         713
Total Negative Acknowledgments                            0           0
                            Device Drivers
Total via Local Driver                                    12          12
Total via Platform Driver                               9478        1619
Total Frames Dropped by Platform Drivers                   0           0
Total Frames Sent when media is quiesced                               0
                    Reliable Tx Statistics
Re-Transmission                                                        0
Re-Tx Timeout                                                          0
         Rx Errors                              Tx Errors
Unsupp IPC Proto Version          0  Tx Session Error                 0
Corrupt Frame                     0  Tx Seat Error                    0
Duplicate Frame                   0  Destination Unreachable          0
Rel Out-of-Seq Frame              0  Unrel Out-of-Seq Frame           0
Dest Port does Not Exist          0  Tx Driver Failed                 0
Rx IPC Msg Alloc Failed           0  Rx IPC Frag Dropped              0
Rx IPC Transform Errors           0  Tx IPC Transform Errors          0
Unable to Deliver Msg             0  Tx Test Drop                     0
Ctrl Frm Alloc Failed             0  Rx Msg Callback Hog             11
         Buffer Errors                          Misc Errors
IPC Msg Alloc                     0  IPC Open Port                    0
Emer IPC Msg Alloc                0  No HWQ                           0
IPC Frame PakType Alloc           0  Hardware Error                   0
IPC Frame MemD Alloc              0  Invalid Messages                 0
         Tx Driver Errors
No Transport                      0
MTU Failure                       0
Dest does not Exist               0
```

Related Commands

Command	Description
show ipc	Displays IPC statistics.

show ipv6 ospf interface

To display Open Shortest Path First (OSPF)-related interface information, use the **showipv6ospfinterface** command in user EXEC or privileged mode.

show ipv6 ospf [*process-id*] [*area-id*] **interface** [*type number*] [**brief**]

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled.
area-id	(Optional) Displays information about a specified area only.
type number	(Optional) Interface type and number.
brief	(Optional) Displays brief overview information for OSPF interfaces, states, addresses and masks, and areas on the router.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.3(4)T	Command output is changed when authentication is enabled.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(9)T	Command output is changed when encryption is enabled.
12.2(33)SRB	The **brief** keyword was added.
12.4(15)XF	Output displays were modified so that VMI PPPoE interface-based local state values are displayed in the command output when a VMI interface is specified.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	Command output was updated to display graceful restart information.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

Release	Modification
15.1(1)SY	This command was was modified. It was integrated into Cisco IOS Release 15.1(1)SY.

Examples

show ipv6 ospf interface Standard Output Example

The following is sample output from the **showipv6ospfinterface** command:

```
Router# show ipv6 ospf interface
ATM3/0 is up, line protocol is up
  Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 13
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Network Type POINT_TO_POINT, Cost: 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  Index 1/2/2, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 12, maximum is 12
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.4.4
  Suppress hello for 0 neighbor(s)
FastEthernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 3
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 172.16.6.6, local address 2001:0DB1:205:5FFF:FED3:6408
  Backup Designated router (ID) 172.16.3.3, local address 2001:0DB1:205:5FFF:FED3:5808
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 12, maximum is 12
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.6.6  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

The table below describes the significant fields shown in the display.

Table 172: show ipv6 ospf interface Field Descriptions

Field	Description
ATM3/0	Status of the physical link and operational status of protocol.
Link Local Address	Interface IPv6 address.
Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3	The area ID, process ID, instance ID, and router ID of the area from which this route is learned.
Network Type POINT_TO_POINT, Cost: 1	Network type and link-state cost.

Field	Description
Transmit Delay	Transmit delay, interface state, and router priority.
Designated Router	Designated router ID and respective interface IP address.
Backup Designated router	Backup designated router ID and respective interface IP address.
Timer intervals configured	Configuration of timer intervals.
Hello	Number of seconds until the next hello packet is sent out this interface.
Neighbor Count	Count of network neighbors and list of adjacent neighbors.

Cisco IOS Release 12.2(33)SRB Example

The following is sample output of the **showipv6ospfinterface** command when the **brief** keyword is entered.

```
Router# show ipv6 ospf interface brief

Interface    PID   Area            Intf ID    Cost  State Nbrs F/C
VL0          6     0               21         65535 DOWN  0/0
Se3/0        6     0               14         64    P2P   0/0
Lo1          6     0               20         1     LOOP  0/0
Se2/0        6     6               10         62    P2P   0/0
Tu0          1000  0               19         11111 DOWN  0/0
```

OSPF with Authentication on the Interface Example

The following is sample output from the **showipv6ospfinterface** command with authentication enabled on the interface:

```
Router# show ipv6 ospf interface
Ethernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:A8BB:CCFF:FE00:6E00, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.10.10.1
  Network Type BROADCAST, Cost:10
  MD5 Authentication SPI 500, secure socket state UP (errors:0)
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.11.11.1, local address 2001:0DB1:A8BB:CCFF:FE00:6F00
  Backup Designated router (ID) 10.10.10.1, local address
2001:0DB1:A8BB:CCFF:FE00:6E00
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.11.11.1  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

OSPF with Null Authentication Example

The following is sample output from the **showipv6ospfinterface** command with null authentication configured on the interface:

```
Router# show ipv6 ospf interface
Ethernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:A8BB:CCFF:FE00:6E00, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.10.10.1
  Network Type BROADCAST, Cost:10
  Authentication NULL
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.11.11.1, local address 2001:0DB1:A8BB:CCFF:FE00:6F00
  Backup Designated router (ID) 10.10.10.1, local address
2001:0DB1:A8BB:CCFF:FE00:6E00
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.11.11.1  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

OSPF with Authentication for the Area Example

The following is sample output from the **showipv6ospfinterface** command with authentication configured for the area:

```
Router# show ipv6 ospf interface
Ethernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:A8BB:CCFF:FE00:6E00, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.10.10.1
  Network Type BROADCAST, Cost:10
  MD5 Authentication (Area) SPI 1000, secure socket state UP (errors:0)
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.11.11.1, local address 2001:0DB1:A8BB:CCFF:FE00:6F00
  Backup Designated router (ID) 10.10.10.1, local address
FE80::A8BB:CCFF:FE00:6E00
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.11.11.1  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

OSPF with Dynamic Cost Example

The following display shows sample output from the **showipv6ospfinterface** command when the OSPF cost dynamic is configured.

```
Router1# show ipv6 ospf interface serial 2/0
```

```
Serial2/0 is up, line protocol is up
   Link Local Address 2001:0DB1:A8BB:CCFF:FE00:100, Interface ID 10
   Area 1, Process ID 1, Instance ID 0, Router ID 172.1.1.1
   Network Type POINT_TO_MULTIPOINT, Cost: 64 (dynamic), Cost Hysteresis: 200
   Cost Weights: Throughput 100, Resources 20, Latency 80, L2-factor 100
   Transmit Delay is 1 sec, State POINT_TO_MULTIPOINT,
   Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
     Hello due in 00:00:19
   Index 1/2/3, flood queue length 0
   Next 0x0(0)/0x0(0)/0x0(0)
   Last flood scan length is 0, maximum is 0
   Last flood scan time is 0 msec, maximum is 0 msec
   Neighbor Count is 0, Adjacent neighbor count is 0
   Suppress hello for 0 neighbor(s)
```

OSPF Graceful Restart Example

The following display shows sample output from the **showipv6ospfinterface** command when the OSPF graceful restart feature is configured:

```
Router# show ipv6 ospf interface
Ethernet0/0 is up, line protocol is up
  Link Local Address FE80::A8BB:CCFF:FE00:300, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.3.3.3
  Network Type POINT_TO_POINT, Cost: 10
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
   Graceful Restart p2p timeout in 00:00:19
    Hello due in 00:00:02
  Graceful Restart helper support enabled
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.1.1.1
  Suppress hello for 0 neighbor(s)
```

Example of an Enabled Protocol

The following display shows that the OSPF interface is enabled for Bidirectional Forwarding Detection (BFD):

```
Router# show ipv6 ospf interface
Serial10/0 is up, line protocol is up
  Link Local Address FE80::A8BB:CCFF:FE00:6500, Interface ID 42
  Area 1, Process ID 1, Instance ID 0, Router ID 10.0.0.1
  Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT, BFD enabled
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.1.0.1
  Suppress hello for 0 neighbor(s)
```

Related Commands

Command	Description
show ipv6 ospf graceful-restart	Displays OSPFv3 graceful restart information.

show l2protocol-tunnel

To display the protocols that are tunneled on an interface or on all interfaces, use the **showl2protocol-tunnel** command.

show l2protocol-tunnel [{**interface** *interface mod/port* | **summary** | **vlan** *vlan*}]

Syntax Description

interface *interface-id*	(Optional) Specifies the interface type; possible valid values are **ethernet**, **FastEthernet**, **gigabitethernet**, **tengigabitethernet**, **pos**, **atm**, and **ge-wan**
mod/port	Module and port number.
summary	(Optional) Displays a summary of a tunneled port.
vlan*vlan*	(Optional) Limits the display to interfaces on the specified VLAN. Valid values are from 1 to 4094.

Command Modes

EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX	The **showl2protocol-tunnelsummary** command output was changed to display the following information: • Global drop-threshold setting • Up status of a Layer 2-protocol interface tunnel
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX release.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXI	This command was changed to add the optional **vlan***vlan* keyword and argument.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

After enabling Layer 2 protocol tunneling on an access or IEEE 802.1Q tunnel port by using the l2protocol-tunnel interface configuration command, you can configure some or all of these parameters:

- Protocol type to be tunneled
- Shutdown threshold
- Drop threshold

The **showl2protocol-tunnel** command displays only the ports that have protocol tunneling enabled.

The **showl2protocol-tunnelsummary** command displays the ports that have protocol tunneling enabled, regardless of whether the port is down or currently configured as a trunk.

Examples

The following example is an output from the show l2protocol-tunnel command:

```
Router# show l2protocol-tunnel
COS for Encapsulated Packets: 5
Drop Threshold for Encapsulated Packets: 0
```

Port	Protocol	Shutdown Threshold	Drop Threshold	Encapsulation Counter	Decapsulation Counter	Drop Counter
Fa0/3	---	----	----	----	----	----
	---	----	----	----	----	----
	---	----	----	----	----	----
	pagp	----	----	0	242500	
	lacp	----	----	24268	242640	
	udld	----	----	0	897960	
Fa0/4	---	----	----	----	----	----
	---	----	----	----	----	----
	---	----	----	----	----	----
	pagp	1000	----	24249	242700	
	lacp	----	----	24256	242660	
	udld	----	----	0	1344820	
Gi0/3	cdp	----	----	134482	1344820	
	---	----	----	----	----	----
	---	----	----	----	----	----
	pagp	1000	----	0	242500	

	lacp	500	----	0	485320	
	udld	300	----	44899	448980	
Gi0/3	cdp	----	----	134482	1344820	
	---	----	----	----	----	----
	---	----	----	----	----	----
	pagp	----	1000	0	242700	
	lacp	----	----	0	485220	
	udld	300	----	44899	448980	

This example shows how to display a summary of Layer 2-protocol tunnel ports:

```
Router# show l2protocol-tunnel summary
COS for Encapsulated Packets:5
Drop Threshold for Encapsulated Packets:0
Port    Protocol    Shutdown         Drop             Status
                    Threshold        Threshold
                    (cdp/stp/vtp)    (cdp/stp/vtp)
------- ----------- ---------------- ---------------- ----------
Fa9/1   --- stp --- ----/----/----   ----/----/----   down
Fa9/9   cdp stp vtp ----/----/----   ----/----/----   up
Fa9/47  --- --- --- ----/----/----   1500/1500/1500   down(trunk)
Fa9/48  cdp stp vtp ----/----/----   ----/----/----   down(trunk)
```

This example shows how to display Layer 2-protocol tunnel information on interfaces for a specific VLAN:

```
Router# show l2protocol-tunnel vlan 1
COS for Encapsulated Packets: 5
Drop Threshold for Encapsulated Packets: 0
Protocol Drop Counter
-------- -------------
 cdp                 0
 lldp                0
 stp                 0
 vtp                 0
Port                Protocol Thresholds          Counters
                             Shutdown  Drop      Encap     Decap     Drop
------------------- -------- --------- --------- --------- --------- ---------
```

Related Commands

Command	Description
debug l2protocol-tunnel	Displays the debugging options for L2PT.
l2protocol-tunnel	Enables the protocol tunneling on an interface and specifies the type of protocol to be tunneled.

Command	Description
l2protocol-tunnel drop-threshold	Specifies the maximum number of packets that can be processed for the specified protocol on that interface before being dropped.
l2protocol-tunnel global drop-threshold	Enables rate limiting at the software level.
l2protocol-tunnel shutdown-threshold	Specifies the maximum number of packets that can be processed for the specified protocol on that interface in 1 second.

show l3-mgr

To display the information about the Layer 3 manager , use the **showl3-mgr** command in user EXEC or privileged EXEC mode.

show l3-mgr status
show l3-mgr {**interface** **interface** **interface-number** | **null** **interface-number** | **port-channel** **number** | **vlan** **vlan-id** | **status**}

Syntax Description

status	Displays information about the global variable.
interface	Displays information about the Layer 3 manager .
interface	Interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **pos**, **atm**, and **ge-wan**.
interface-number	Module and port number; see the “Usage Guidelines” section for valid values.
null *interface-number*	Specifies the null interface; the valid value is **0**.
port-channel *number*	Specifies the channel interface; valid values are a maximum of 64 values ranging from 1 to 282.
vlan *vlan-id*	Specifies the VLAN; valid values are from 1 to 4094.
status	Displays status information about the Layer 3 manager.

Command Default

This command has no default settings.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

The **port-channel***number*values from 257 to 282 are supported on the CSM and the FWSM only.

Examples

This example shows how to display the status of the Layer 3 manager:

```
Router#
```

```
show l3-mgr status
l3_mgr_state:         2
l3_mgr_req_q.count:   0
l3_mgr_req_q.head:    0
l3_mgr_req_q.tail:    0
l3_mgr_max_queue_count:  1060
l3_mgr_shrunk_count:  0
l3_mgr_req_q.ip_inv_count:    303
l3_mgr_req_q.ipx_inv_count:   0
l3_mgr_outpak_count:  18871
l3_mgr_inpak_count:   18871
l3_mgr_max_pending_pak: 4
l3_mgr_pending_pak_count: 0
nde enable statue:    0
current nde addr:     0.0.0.0
Router#
```

This example shows how to display the information about the Layer 3 manager for a specific interface:

```
Router#
show l3-mgr interface fastethernet 5/40
vlan:                 0
ip_enabled:         1
ipx_enabled:        1
bg_state:           0 0 0 0
hsrp_enabled:       0
hsrp_mac:           0000.0000.0000
state:              0
up:                 0
Router#
```

show l3vpn encapsulation ip

To display the L3VPN encapsulation profile health and the underlying tunnel interface, use the **showl3vpnencapsulationip** command in privileged EXEC mode.

show l3vpn encapsulation ip [*profile name*]

Syntax Description

profile name	(Optional) Name of the Layer 3 encapsulation profile.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.

Examples

The following is a sample output from the **showl3vpnencapsulationip** command:

```
Router# show l3vpn encapsulation ip tunnelencap
Profile: tunnelencap
    transport ipv4 source Loopback0
    protocol gre key 500
  Tunnel Tunnel0 Created [OK]
  Tunnel Linestate
  Tunnel Transport Source Loopback0
```

show lacp

To display Link Aggregation Control Protocol (LACP) and multi-chassis LACP (mLACP) information, use the **show lacp** command in either user EXEC or privileged EXEC mode.

show lacp {*channel-group-number* {**counters** | **internal** [**detail**] | **neighbor** [**detail**]} | **multi-chassis** [**load-balance**] {**group** *number* | **port-channel** *number*} | **sys-id**}

Cisco ASR 901 Series Aggregation Services Router

show lacp {*channel-group-number* {**counters** | **internal** [**detail**] | **neighbor** [**detail**] | **sys-id**}}

Syntax Description

channel-group- number	(Optional) Number of the channel group. The following are valid values: • Cisco IOS 12.2 SB and Cisco IOS XE 2.4 Releases--from 1 to 64 • Cisco IOS 12.2 SR Releases--from 1 to 308 • Cisco IOS 12.2 SX Releases--from 1 to 496 • Cisco IOS 15.1S Releases—from 1 to 564 • Cisco ASR 901 Series Aggregation Services Router—from 1 to 8
counters	Displays information about the LACP traffic statistics.
internal	Displays LACP internal information.
neighbor	Displays information about the LACP neighbor.
detail	(Optional) Displays detailed internal information when used with the **internal** keyword and detailed LACP neighbor information when used with the **neighbor** keyword.
multi-chassis	Displays information about mLACP.
load-balance	Displays mLACP load balance information.
group	Displays mLACP redundancy group information,
number	Integer value used with the **group** and **port-channel** keywords. • Values from 1 to 4294967295 identify the redundancy group. • Values from 1 to 564 identify the port-channel interface.
port-channel	Displays mLACP port-channel information.
sys-id	Displays the LACP system identification. It is a combination of the port priority and the MAC address of the device

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	Support for this command on the Cisco 7600 router was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4.
12.2(33)SRE	This command was modified. The **multi-chassis**, **group**, and **port-channel**keywords and *number* argument were added.
15.1(3)S	This command was modified. The **load-balance** keyword was added.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

Use the **show lacp** command to troubleshoot problems related to LACP in a network.

If you do not specify a value for the argument *channel-group-number*, all channel groups are displayed. Values in the range of 257 to 282 are supported on the CSM and the FWSM only.

Examples

show lacp sys-id Example

This example shows how to display the LACP system identification using the **show lacp sys-id**command:

```
Device> show lacp sys-id
```

```
8000,AC-12-34-56-78-90
```

The system identification is made up of the system priority and the system MAC address. The first two bytes are the system priority, and the last six bytes are the globally administered individual MAC address that is associated to the system.

LACP Statistics for a Specific Channel Group Examples

This example shows how to display the LACP statistics for a specific channel group:

```
Device# show lacp 1 counters
```

```
              LACPDUs         Marker       LACPDUs
Port       Sent   Recv     Sent   Recv     Pkts Err
---------------------------------------------------
Channel group: 1
```

```
  Fa4/1    8       15       0       0          3    0
  Fa4/2    14      18       0       0          3    0
  Fa4/3    14      18       0       0          0
  Fa4/4    13      18       0       0          0
```

The output displays the following information:

- The LACPDUs Sent and Recv columns display the LACPDUs that are sent and received on each specific interface.
- The LACPDUs Pkts and Err columns display the marker-protocol packets.

The following example shows output from a **show lacp***channel-group-number***counters**command:

```
Device1# show lacp 5 counters

             LACPDUs         Marker      Marker Response    LACPDUs
Port       Sent   Recv     Sent   Recv     Sent   Recv      Pkts Err
---------------------------------------------------------------------
Channel group: 5
Gi5/0/0     21     18        0      0        0      0          0
```

The following table describes the significant fields shown in the display.

Table 173: show lacp channel-group-number counters Field Descriptions

Field	Description
LACPDUs Sent Recv	Number of LACP PDUs sent and received.
Marker Sent Recv	Attempts to avoid data loss when a member link is removed from an LACP bundle.
Marker Response Sent Recv	Cisco IOS response to the Marker protocol.
LACPDUs Pkts Err	Number of LACP PDU packets transmitted and the number of packet errors.

The following example shows output from a **show lacp internal**command:

```
Device1# show lacp 5 internal

Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode
Channel group 5
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
Gi5/0/0   SA      bndl      32768         0x5       0x5     0x42        0x3D
```

The following table describes the significant fields shown in the display.

Table 174: show lacp internal Field Descriptions

Field	Description
Flags	Meanings of each flag value, which indicates a device activity.
Port	Port on which link bundling is configured.

Field	Description
Flags	Indicators of device activity.
State	Activity state of the port. States can be any of the following: • Bndl--Port is attached to an aggregator and bundled with other ports. • Susp--Port is in suspended state, so it is not attached to any aggregator. • Indep--Port is in independent state (not bundled but able to switch data traffic). This condition differs from the previous state because in this case LACP is not running on the partner port. • Hot-sby--Port is in hot standby state. • Down--Port is down.
LACP port Priority	Priority assigned to the port.
Admin Key	Defines the ability of a port to aggregate with other ports.
Oper Key	Determines the aggregation capability of the link.
Port Number	Number of the port.
Port State	State variables for the port that are encoded as individual bits within a single octet with the following meaning: • bit0: LACP_Activity • bit1: LACP_Timeout • bit2: Aggregation • bit3: Synchronization • bit4: Collecting • bit5: Distributing • bit6: Defaulted • bit7: Expired

Internal Information About a Specific Channel Group Example

This example shows how to display internal information for the interfaces that belong to a specific channel:

```
Device# show lacp 1 internal

Flags:  S - Device sends PDUs at slow rate. F - Device sends PDUs at fast rate.
        A - Device is in Active mode.       P - Device is in Passive mode.
Channel group 1
                            LACPDUs     LACP Port    Admin   Oper    Port     Port
```

```
Port      Flags    State    Interval    Priority     Key     Key     Number   State
Fa4/1     saC      bndl     30s         32768        100     100     0xc1     0x75
Fa4/2     saC      bndl     30s         32768        100     100     0xc2     0x75
Fa4/3     saC      bndl     30s         32768        100     100     0xc3     0x75
Fa4/4     saC      bndl     30s         32768        100     100     0xc4     0x75
Device#
```

The following table describes the significant fields shown in the display.

Table 175: show lacp internal Field Descriptions

Field	Description
State	Current state of the port; allowed values are as follows: • bndl--Port is attached to an aggregator and bundled with other ports. • susp--Port is in a suspended state; it is not attached to any aggregator. • indep--Port is in an independent state (not bundled but able to switch data traffic. In this case, LACP is not running on the partner port). • hot-sby--Port is in a hot-standby state. • down--Port is down.
LACPDUs Interval	Interval setting.
LACP Port Priority	Port-priority setting.
Admin Key	Defines the ability of a port to aggregate with other ports.
Oper Key	Determines the aggregation capability of the link.
Port Number	Port number.
Port State	Activity state of the port. • See the Port State description in the show lacp internal Field Descriptions table for state variables.

Information About LACP Neighbors for a Specific Port Example

This example shows how to display the information about the LACP neighbors for a specific port channel:

```
Device# show lacp 1 neighbors

Flags:  S - Device sends PDUs at slow rate. F - Device sends PDUs at fast rate.
        A - Device is in Active mode.       P - Device is in Passive mode.
Channel group 1 neighbors
          Partner                  Partner
Port      System ID                Port Number     Age     Flags
Fa4/1     8000,00b0.c23e.d84e      0x81            29s     P
Fa4/2     8000,00b0.c23e.d84e      0x82            0s      P
Fa4/3     8000,00b0.c23e.d84e      0x83            0s      P
Fa4/4     8000,00b0.c23e.d84e      0x84            0s      P
```

```
         Port         Admin     Oper      Port
         Priority     Key       Key       State
Fa4/1    32768        200       200       0x81
Fa4/2    32768        200       200       0x81
Fa4/3    32768        200       200       0x81
Fa4/4    32768        200       200       0x81
Device#
```

The following table describes the significant fields shown in the display.

Table 176: show lacp neighbors Field Descriptions

Field	Description
Port	Port on which link bundling is configured.
Partner System ID	Peer's LACP system identification (sys-id). It is a combination of the system priority and the MAC address of the peer device.
Partner Port Number	Port number on the peer device
Age	Number of seconds since the last LACP PDU was received on the port.
Flags	Indicators of device activity.
Port Priority	Port priority setting.
Admin Key	Defines the ability of a port to aggregate with other ports.
Oper Key	Determines the aggregation capability of the link.
Port State	Activity state of the port. See the Port State description in the show lacp internal Field Descriptions table for state variables.

If no PDUs have been received, the default administrative information is displayed in braces.

Related Commands

Command	Description
clear lacp counters	Clears the statistics for all interfaces belonging to a specific channel group.
lacp port-priority	Sets the priority for the physical interfaces.
lacp system-priority	Sets the priority of the system.

show link state group

To display the link-state group information., use the **showlinkstategroup** command in user EXEC or privileged EXEC mode .

show link state group detail

Syntax Description

detail	Displays the detailed information about the group.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)S	This command was introduced.

Usage Guidelines

Link State Ttracking (LST), also known as trunk failover, is a feature that binds the link state of multiple interfaces. When you configure LST for the first time, add upstream interfaces to the link state group before adding the downstream interface, otherwise the downstream interfaces would move into error-disable mode. The maximum number of link state groups configurable is 10.

Examples

The following example displays the link-state group information:

```
Router# enable
Router# show link state group 1
Link State Group: 1 Status: Enabled, Down
Router> show link state group detail
(Up):Interface up (Dwn):Interface Down (Dis):Interface disabled
Link State Group: 1 Status: Enabled, Down
Upstream Interfaces : Gi3/5(Dwn) Gi3/6(Dwn)
Downstream Interfaces : Gi3/1(Dis) Gi3/2(Dis) Gi3/3(Dis) Gi3/4(Dis)
Link State Group: 2 Status: Enabled, Down
Upstream Interfaces : Gi3/15(Dwn) Gi3/16(Dwn) Gi3/17(Dwn)
Downstream Interfaces : Gi3/11(Dis) Gi3/12(Dis) Gi3/13(Dis) Gi3/14(Dis)
(Up):Interface up (Dwn):Interface Down (Dis):Interface disabled
```

Related Commands

Command	Description
link state track	Configures the link state tracking number.
link state group	Configures the link state group and interface, as either an upstream or downstream interface in the group.

show mac-address-table dynamic

To display dynamic MAC address table entries only, use the **showmac-address-tabledynamic** command in privileged EXEC mode.

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

show mac-address-table dynamic [{**address** *mac-addr* | **interface** *interface type slot/number* | **vlan** *vlan*}]

Catalyst Switches

show mac-address-table dynamic [{**address** *mac-addr* | **detail** | **interface** *interface number***protocol** *protocol* | **module** *number* | **vlan** *vlan*}][{**begin** | **exclude** | **include***expression*}]

Catalyst 6500 Series Switches

show mac-address-table dynamic [{**address** *mac-addr* | **interface** *interface interface-number* [{**all** | **module** *number*}] | **module** *num* | **vlan** *vlan-id* [{**all** | **module** *number*}]}]

Syntax Description

address *mac -address*	(Optional) Specifies a 48-bit MAC address; valid format is H.H.H.
detail	(Optional) Specifies a detailed display of MAC address table information.
interface *type number*	(Optional) Specifies an interface to match; valid type values are FastEthernet and GigabitEthernet, valid number values are from 1 to 9.
interface *type*	(Optional) Specifies an interface to match; valid type values are FastEthernet and GigabitEthernet.
slot	(Optional) Adds dynamic addresses to module in slot 1 or 2.
port	(Optional) Port interface number ranges based on type of Ethernet switch network module used: • 0 to 15 for NM-16ESW • 0 to 35 for NM-36ESW • 0 to 1 for GigabitEthernet
protocol *protocol*	(Optional) Specifies a protocol. See the "Usage Guidelines" section for keyword definitions.
module *number*	(Optional) Displays information about the MAC address table for a specific Distributed Forwarding Card (DFC) module.
vlan *vlan*	(Optional) Displays entries for a specific VLAN; valid values are from 1 to 1005.
begin	(Optional) Specifies that the output display begin with the line that matches the expression.
exclude	(Optional) Specifies that the output display exclude lines that match the expression.

include	(Optional) Specifies that the output display include lines that match the specified expression.
expression	Expression in the output to use as a reference point.
all	(Optional) Specifies that the output display all dynamic MAC-address table entries.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(7)XE	This command was introduced on Catalyst 6000 series switches.
12.2(2)XT	This command was implemented on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(14)SX	Support for this command was introduced on the Catalyst 6500 series switch.
12.2(33)SXH	This command was changed to support the **all** keyword on the Catalyst 6500 series switch.

Usage Guidelines

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

The **showmac-address-tabledynamic** command output for an EtherChannel interface changes the port-number designation (for example, 5/7) to a port-group number.

Catalyst Switches

The keyword definitions for the protocol argument are:

- **ip** --Specifies IP protocol
- **ipx** --Specifies Internetwork Packet Exchange (IPX) protocols
- **assigned** --Specifies assigned protocol entries
- **other** --Specifies other protocol entries

The **showmac-address-tabledynamic** command output for an EtherChannel interface changes the port-number designation (for example, 5/7) to a port-group number.

Catalyst 6500 Series Switches

The *mac-address*is a 48-bit MAC address and the valid format is H.H.H.

The optional **module***num* keyword and argument are supported only on DFC modules. The **module***num*keyword and argument designate the module number.

Examples

The following examples show how to display all dynamic MAC address entries. The fields shown in the various displays are self-explanatory.

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

```
Router# show mac-address-table dynamic

Non-static Address Table:
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
000a.000a.000a          Dynamic       1     FastEthernet4/0
002a.2021.4567          Dynamic       2     FastEthernet4/0
```

Catalyst Switches

```
Router# show mac-address-table dynamic
vlan   mac address     type    protocol  qos             ports
-----+---------------+--------+---------+---+--------------------------------
 200  0010.0d40.37ff  dynamic        ip  --  5/8
   1  0060.704c.73ff  dynamic        ip  --  5/9
4095  0000.0000.0000  dynamic        ip  --  15/1
   1  0060.704c.73fb  dynamic     other  --  5/9
   1  0080.1c93.8040  dynamic        ip  --  5/9
4092  0050.f0ac.3058  dynamic        ip  --  15/1
   1  00e0.4fac.b3ff  dynamic     other  --  5/9
```

The following example shows how to display dynamic MAC address entries with a specific protocol type (in this case, assigned).

```
Router# show mac-address-table dynamic protocol assigned
vlan   mac address     type    protocol  qos             ports
-----+---------------+--------+---------+---+--------------------------------
4092  0000.0000.0000  dynamic  assigned  --  Router
4092  0050.f0ac.3059  dynamic  assigned  --  Router
   1  0010.7b3b.0978  dynamic  assigned  --  Fa5/9
Router#
```

The following example shows the detailed output for the previous example.

```
Router# show mac-address-table dynamic protocol assigned detail
MAC Table shown in details
========================================
 Type   Always Learn Trap Modified Notify Capture Protocol Flood
-------+------------+----+--------+------+-------+--------+-----+
     QoS bit      L3 Spare   Mac Address  Age Byte Pvlan Xtag SWbits Index
-----------------+--------+--------------+--------+-----+----+------+-----
DYNAMIC     NO        NO     YES     NO     NO    assigned   NO
   Bit Not On        0     0000.0000.0000  255      4092   0     0     0x3

DYNAMIC     NO        NO     YES     NO     NO    assigned   NO
   Bit Not On        0     0050.f0ac.3059  254      4092   0     0     0x3

DYNAMIC     NO        NO     YES     NO     NO    assigned   NO
   Bit Not On        0     0010.7b3b.0978  254      1      0     0     0x108

Router#
```

Catalyst 6500 Series Switches

This example shows how to display all the dynamic MAC-address entries for a specific VLAN.

```
Router# show mac-address-table dynamic vlan 200 all
Legend: * - primary entry
        age - seconds since last seen
        n/a - not aevailable
vlan     mac address      type   learn    age               ports
------+----------------+--------+-----+----------+--------------------------
 200  0010.0d40.37ff   dynamic    NO      23        Gi5/8
Router#
```

This example shows how to display all the dynamic MAC-address entries.

```
Router# show mac-address-table dynamic
Legend: * - primary entry
age - seconds since last seen
n/a - not applicable
vlan     mac address      type   learn    age               ports
------+----------------+--------+-----+----------+--------------------------
* 10   0010.0000.0000   dynamic  Yes   n/a        Gi4/1
* 3    0010.0000.0000   dynamic  Yes   0          Gi4/2
* 1    0002.fcbc.ac64   dynamic  Yes   265        Gi8/1
* 1    0009.12e9.adc0   static   No    -          Router
Router#
```

Related Commands

Command	Description
show mac -address-tableaddress	Displays MAC address table information for a specific MAC address.
show mac -address-tableaging-time	Displays the MAC address aging time.
show mac -address-tablecount	Displays the number of entries currently in the MAC address table.
show mac -address-tabledetail	Displays detailed MAC address table information.
show mac -address-tableinterface	Displays the MAC address table information for a specific interface.
show mac -address-tablemulticast	Displays multicast MAC address table information.
show mac -address-tableprotocol	Displays MAC address table information based on protocol.
show mac -address-tablestatic	Displays static MAC address table entries only.
show mac -address-tablevlan	Displays the MAC address table information for a specific VLAN.

show mls asic

To display the application-specific integrated circuit (ASIC) version, use the **showmlsasic** command in user EXEC or privileged EXEC mode.

show mls asic

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to display the ASIC versions on a Supervisor Engine 2:

```
Router#
show mls asic
  Cafe version: 2
  Centauri version: 1
  Perseus version: 0/0
  Titan version: 1
Router#
```

This example shows how to display the ASIC versions on a Supervisor Engine 720:

```
Router#
show mls asic
Earl in Module 2
 Tycho - ver:1 Cisco-id:1C8 Vendor-id:49
Router#
```

Related Commands

Command	Description
show mls df-table	Displays information about the DF table.
show mls ip	Displays the Multilayer Switching (MLS) IP information.
show mls ipx	Displays the Multilayer Switching (MLS) IPX information.
show mls qos	Displays Multilayer Switching (MLS) quality of service (QoS) information
show mls statistics	Displays the Multilayer Switching (MLS) statistics for the Internet Protocol (IP)

show mls ip

To display the Multilayer Switching (MLS) IP information, use the **showmlsip** command in user EXEC or privileged EXEC mode.

show mls ip [{**any** | **destination** {*hostnameip-address*} | **detail** | **flow** {**tcp** | **udp**} | {**vlan** *vlan-id* | **macd** *destination-mac-address* | **macs** *source-mac-address* | **module** *number* | **source** {*hostnameip-address*}} | **count** | **static**}]
show mls ip {**ipv6** | **mpls**}

Syntax Description

any	(Optional) Displays any MLS IP information.
destination *hostname*	(Optional) Displays the entries for a specific destination hostname.
destination *ip-address*	(Optional) Displays the entries for a specific destination IP address.
detail	(Optional) Specifies a detailed output.
flow	(Optional) Specifies the flow type.
tcp | **udp**	Selects the flow type.
vlan *vlan-id*	(Optional) Specifies the virtual local area network (VLAN) ID; valid values are from 1 to 4094.
macd *destination-mac-address*	(Optional) Specifies the destination MAC address.
macs *source- mac-address*	(Optional) Specifies the source Media Access Control (MAC) address.
module *number*	(Optional) Displays the entries that are downloaded on the specified module; see the "Usage Guidelines" section for valid values.
source *hostname*	(Optional) Displays the entries for a specific source address.
source *ip-address*	(Optional) Displays the entries for a specific source IP address.
count	(Optional) Displays the total number of MLS entries.
static	(Optional) Displays the total number of static entries.
ipv6	Displays the total number of IPv6 entries.
mpls	Displays the total number of MPLS entries.

Command Default

This command has no default settings.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.

Release	Modification
12.2(17a)SX	This command is supported on releases prior to Release 12.2(17a)SX only.
12.2(17b)SXA	On Cisco 7600 series routers that are configured with a Supervisor Engine 720, this command is replaced by the show mls netflow ip command.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **static**, **ipv6** and **mpls** keywords are not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48. This definition also applies to the **module***number* keyword and argument.

When you view the output, note that a colon (:) is used to separate the fields.

Examples

This example shows how to display any MLS IP information:

```
Router#
show mls ip
 any
Displaying Netflow entries in Supervisor Earl
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f:AdjPtr
--------------------------------------------------------------------
Pkts         Bytes         Age   LastSeen  Attributes
---------------------------------------------------
0.0.0.0         0.0.0.0         0   :0      :0        0   : 0x0
82           3772          1329  20:46:03   L3 - Dynamic
Router#
```

This example shows how to display MLS information on a specific IP address:

```
Router#
show mls ip
 destination 172.20.52.122
Displaying Netflow entries in Supervisor Earl
DstIP           SrcIP           Dst i/f:DstMAC       Pkts         Bytes
-----------------------------------------------------------------------
SrcDstPorts   SrcDstEncap Age   LastSeen
----------------------------------------
172.20.52.122   0.0.0.0         5   : 00e0.4fac.b3ff 684          103469
Fa5/9,Fa5/9 ARPA,ARPA   281   07:17:02
 Number of Entries Found = 1
Router#
```

This example shows how to display MLS information on a specific flow type:

```
Router# show mls ip
 flow udp
```

```
Displaying Netflow entries in Supervisor Earl
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f:AdjPtr
--------------------------------------------------------------------
Pkts         Bytes         Age   LastSeen  Attributes
---------------------------------------------------
0.0.0.0         0.0.0.0         0   :0      :0        0   : 0x0
78           3588          1259  20:44:53   L3 - Dynamic
Router#
```

This example shows how to display detailed MLS information:

```
Router#
 show mls ip
 detail
Displaying Netflow entries in Supervisor Earl
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f:AdjPtr
--------------------------------------------------------------------
Pkts         Bytes         Age   LastSeen  Attributes
---------------------------------------------------
Mask Pi R CR Xt Prio Dsc IP_EN OP_EN Pattern Rpf FIN_RDT FIN/RST
----+--+-+--+--+----+---+-----+-----+-------+---+-------+-------
Ig/acli Ig/aclo Ig/qosi Ig/qoso Fpkt Gemini MC-hit Dirty Diags
-------+-------+-------+-------+----+------+------+-----+------
    QoS     Police Count Threshold    Leak     Drop Bucket  Use-Tbl Use-Enable
-----------+------------+---------+-----------+----+-------+-------+----------+
127.0.0.19      127.0.0.16      udp :68     :67       1009: 0x0
72           3312          1170  20:43:24   L3 - Dynamic
0    1  0  0  1  0    0    1     1     0       0     0      0
0          0       0       0      0    0       0     0     0
  0x0          0               0        0       NO   64        NO       NO
Router#
```

Related Commands

Command	Description
show mls asic	display the application-specific integrated circuit (ASIC) version
show mls df-table	Displays information about the DF table.
show mls ipx	Displays the Multilayer Switching (MLS) IPX information.
show mls qos	Displays Multilayer Switching (MLS) quality of service (QoS) information
show mls statistics	Displays the Multilayer Switching (MLS) statistics for the Internet Protocol (IP)

show mls ipx

To display Multilayer Switching (MLS) Internetwork Packet Exchange (IPX) information, use the **showmlsipx** command in user EXEC or privileged EXEC mode.

show mls ipx [{**destination** *ipx-network* | **interface** *interface interface-number* | **vlan** *vlan-id* | **macd** *destination-mac-address* | **macs** *source-mac-address* | **module** *number* | **source** *hostnameipx-network*}] [{**detail** | **count**}]

Syntax Description

destination *ipx-network*	(Optional) Displays the entries for a specific destination network address.
interface	(Optional) Specifies the interface.
interface	(Optional) Interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **pos**, **atm**, and **ge-wan**.
interface-number	(Optional) Module and port number; see the “Usage Guidelines” section for valid values.
vlan *vlan-id*	(Optional) Specifies the virtual local area network (VLAN) ID; valid values are from 1 to 4094.
macd *destination-mac-address*	(Optional) Specifies the destination Media Access Control (MAC) address.
macs *source- mac-address*	(Optional) Specifies the source MAC address.
module *number*	(Optional) Displays the entries that are downloaded on the specified slot; see the “Usage Guidelines” section for valid values.
source *hostname*	(Optional) Displays the entries for a specific source address.
source *ipx-network*	(Optional) Displays the entries for a specific destination network address.
detail	(Optional) Displays the detailed list of entries.
count	(Optional) Displays the total number of MLS entries.

Command Default

This command has no default settings.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720 with a PFC2.

When you enter the *ipx-network* value, the format is N.H.H.H.

When you enter the *destination-mac-address* value, the format for the 48-bit MAC address is H.H.H.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48. These valid values also apply when entering the **module***number* keyword and argument.

Examples

This example shows how to display MLS IPX information:

```
Router#
show mls ipx
DstNet-DstNode          SrcNet   Dst i/f:DstMAC      Pkts         Bytes
-----------------------------------------------------------------------
SrcDstPorts   SrcDstEncap Age   LastSeen
----------------------------------------
 Number of Entries Found = 0
Router#
```

This example shows how to display the total number of MLS entries:

```
Router#
show mls ipx
 count
Number of shortcuts = 66
Router#
```

Related Commands

Command	Description
mls ipx	Enables MLS IPX on the interface.
show mls asic	display the application-specific integrated circuit (ASIC) version
show mls df-table	Displays information about the DF table.
show mls ip	Displays the Multilayer Switching (MLS) IP information.
show mls qos	Displays Multilayer Switching (MLS) quality of service (QoS) information
show mls statistics	Displays the Multilayer Switching (MLS) statistics for the Internet Protocol (IP)

show mobility

To display information about the Layer 3 mobility and the wireless network, use the **showmobility** command in privileged EXEC mode.

show mobility {**ap** [*ip-address*] | **mn** [**ip** *ip-address*] | **mac** *mac-address* | **network** *network-id* | **status**}

Syntax Description

ap	Displays information about the access point.
ip-address	(Optional) IP address.
mn	Displays information about the mobile node.
ip *ip-address*	(Optional) Displays information about the IP database thread.
mac *mac-address*	Displays information about the MAC database thread.
network *network-id*	Displays information for a specific wireless network ID.
status	Displays status information.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXD	This command was introduced on the Supervisor Engine 720.
12.2(18)SXD3	The output of this command was changed to include the TCP adjust-mss status.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported on Cisco 7600 series routers that are configured with a WLSM only.

Examples

This example shows how to display information about the access point:

```
Router# show mobility
 ap
AP IP Address   AP Mac Address Wireless Network-ID
--------------- -------------- -------------------
10.1.1.2 000d.29a2.a852 101 102 109 103
```

This example shows how to display information about the access points for a specific network ID:

```
Router# show mobility
 ap 172.16.1.2 detail
IP Address : 172.16.1.2
MAC Address : 000d.29a2.a852
Participating Wireless Tunnels: 101, 102, 109, 103
Registered Mobile Nodes on AP {172.16.1.2, 000d.29a2.a852} :
MN Mac Address MN IP Address AP IP Address Wireless Network-ID
-------------- --------------- --------------- -------------------
000a.8afa.85c9 10.1.3.11 172.16.1.2 103
```

```
000d.bdb7.83f7 10.1.2.11 172.16.1.2 102
000d.bdb7.83fb 10.1.1.11 172.16.1.2 101
Router# show mobility
 network-id 101
Wireless Network ID : 101
Wireless Tunnel Source IP Address : 10.1.1.1
Wireless Network Properties : Trusted
Wireless Network State : Up
Registered Access Point on Wireless Network 101:
AP IP Address AP Mac Address Wireless Network-ID
--------------- -------------- -------------------
176.16.1.2 000d.29a2.a852 101 102 109 103
Registered Mobile Nodes on Wireless Network 101:
MN Mac Address MN IP Address AP IP Address Wireless Network-ID
-------------- --------------- --------------- -------------------
000d.bdb7.83fb 10.1.1.11 176.16.1.2 101
Router# show mobility
 status
WLAN Module is located in Slot: 4 (HSRP State: Active) LCP
Communication status      : up
MAC address used for Proxy ARP: 0030.a349.d800
Number of Wireless Tunnels    : 1
Number of Access Points       : 2
Number of Mobile Nodes        : 0
Wireless Tunnel Bindings:
Src IP Address   Wireless Network-ID  Flags
---------------  -------------------  -------
10.1.1.1          101                  B
Flags: T=Trusted, B=IP Broadcast enabled, A=TCP Adjust-mss enabled
```

Related Commands

Command	Description
mobility	Configures the wireless mGRE tunnels.

show module

To display the module status and information, use the **show** module command in user EXEC or privileged EXEC mode.

show module [{**mod-num** | **all** | **provision** | **version**}]

Syntax Description

mod -num	(Optional) Number of the module.
all	(Optional) Displays the information for all modules.
provision	(Optional) Displays the status about the module provisioning.
version	(Optional) Displays the version information.

Command Default

This command has no default settings.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

In the Mod Sub-Module fields, the **show module** command displays the supervisor engine number but appends the uplink daughter card's module type and information.

Entering the **show module** command with no arguments is the same as entering the **show module all** command.

Examples

This example shows how to display information for all modules on a Cisco 7600 series router that is configured with a Supervisor Engine 720:

```
Router#
show module

Mod Ports Card Type Model Serial No.
--- ----- -------------------------------------- ------------------ -----------
1 48 CEF720 48 port 10/100/1000mb Ethernet WS-X6748-GE-TX SAL0843557C
2 48 48-port 10/100/1000 RJ45 EtherModule WS-X6148A-GE-45AF SAL1109HZW9
3 48 48-port 10/100/1000 RJ45 EtherModule WS-X6148A-GE-45AF SAL1114KYZ7
4 48 48 port 10/100 mb RJ45 WS-X6348-RJ-45 SAL0543DGZ1
6 2 Supervisor Engine 720 (Active) WS-SUP720-3B SAL1016KASS
7 48 48-port 10/100 mb RJ45 WS-X6148-45AF SAL08321X1H
8 4 CEF720 4 port 10-Gigabit Ethernet WS-X6704-10GE SAL08528ADQ
9 48 48-port 100FX SFP Ethernet Module WS-X6148-FE-SFP SAD090208MB
Mod MAC addresses Hw Fw Sw Status
--- ---------------------------------- ------ ------------ ------------ -------
1 0012.005c.86e0 to 0012.005c.870f 2.1 12.2(14r)S5 12.2(33)SXH Ok
2 001b.0ce4.9fb0 to 001b.0ce4.9fdf 2.2 8.4(1) 8.7(0.22)SXH Ok
```

```
3 001b.534f.0540 to 001b.534f.056f 2.2 8.4(1) 8.7(0.22)SXH Ok
4 0007.4f6c.69f8 to 0007.4f6c.6a27 5.0 5.4(2) 8.7(0.22)SXH Ok
6 0017.9441.44cc to 0017.9441.44cf 5.2 8.4(2) 12.2(33)SXH Ok
7 0011.bb0e.c260 to 0011.bb0e.c28f 1.1 5.4(2) 8.7(0.22)SXH Ok
8 0012.da89.a43c to 0012.da89.a43f 2.0 12.2(14r)S5 12.2(33)SXH Ok
9 0030.f273.baf0 to 0030.f273.bb1f 3.0 8.4(1) 8.7(0.22)SXH Ok
Mod Sub-Module Model Serial Hw Status
---- --------------------------- ------------------ ----------- ------- -------
1 Centralized Forwarding Card WS-F6700-CFC SAL08363HL6 2.0 Ok
2 IEEE Voice Daughter Card WS-F6K-48-AF SAL1108HRB1 2.3 Ok
3 IEEE Voice Daughter Card WS-F6K-48-AF SAL1114KV3P 2.3 Ok
4 Inline Power Module WS-F6K-VPWR 1.0 Ok
6 Policy Feature Card 3 WS-F6K-PFC3B SAL1015K00Q 2.3 Ok
6 MSFC3 Daughterboard WS-SUP720 SAL1016KBY3 2.5 Ok
7 IEEE Voice Daughter Card WS-F6K-FE48-AF SAL08311GGL 1.1 Ok
8 Centralized Forwarding Card WS-F6700-CFC SAL0902040K 2.0 Ok
Mod Online Diag Status
---- -------------------
1 Bypass
2 Bypass
3 Bypass
4 Bypass
6 Bypass
7 Bypass
8 Bypass
9 Bypass
Router#
```

This example shows how to display information for a specific module:

```
Router#
show module 2
Mod Ports Card Type                              Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
  5     2 Supervisor Engine 720 (Active)         WS-SUP720-BASE     SAD0644030K
Mod MAC addresses                       Hw    Fw           Sw           Status
--- ---------------------------------- ------ ------------ ------------ -------
  5 00e0.aabb.cc00 to 00e0.aabb.cc3f   1.0    12.2(2003012 12.2(2003012 Ok
Mod Sub-Module                  Model           Serial           Hw     Status
--- --------------------------- --------------- --------------- ------- -------
  5 Policy Feature Card 3       WS-F6K-PFC3     SAD0644031P     0.302   Ok
  5 MSFC3 Daughtercard          WS-SUP720       SAD06460172     0.701
Mod Online Diag Status
--- -------------------
  5 Not Available
Router#
```

This example shows how to display version information:

```
Router#
show module version

Mod Port Model              Serial #    Versions
--- ---- ------------------ ----------- --------------------------------------
  2 0    WS-X6182-2PA                   Hw : 1.0
                     Fw : 12.2(20030125:231135)
                     Sw : 12.2(20030125:231135)
  4 16   WS-X6816-GBIC      SAD04400CEE Hw : 0.205
         WS-F6K-DFC3A       SAD0641029Y Hw : 0.501
                     Fw : 12.2(20020828:202911)
                     Sw : 12.2(20030125:231135)
  6 2    WS-X6K-SUP3-BASE   SAD064300GU Hw : 0.705
                     Fw : 7.1(0.12-Eng-02)TAM
```

```
                     Sw : 12.2(20030125:231135)
                     Sw1: 8.1(0.45)KIS
         WS-X6K-SUP3-PFC3   SAD064200VR Hw : 0.701
                     Fw : 12.2(20021016:001154)
                     Sw : 12.2(20030125:231135)
         WS-F6K-PFC3        SAD064300M7 Hw : 0.301
  9 48   WS-X6548-RJ-45     SAD04490BAC Hw : 0.301
                     Fw : 6.3(1)
                     Sw : 7.5(0.30)CFW11
Router#
```

This example shows how to display module provisioning information:

```
Router# show module provision
Module Provision
  1    dynamic
  2    dynamic
  3    dynamic
  4    dynamic
  5    dynamic
  6    dynamic
  7    dynamic
  8    dynamic
  9    dynamic
 10    dynamic
 11    dynamic
 12    dynamic
 13    dynamic
Router#
```

Related Commands

Command	Description
show interfaces	Displays the status and statistics for the interfaces in the chassis.
show environment alarm	Displays the information about the environmental alarm.
show fm summary	Displays a summary of FM Information.
show environment status	Displays the information about the operational FRU status.

show msfc

To display Multilayer Switching Feature Card (MSFC) information, use the **show msfc** command in user EXEC or privileged EXEC mode.

show msfc {**buffers** | **eeprom** | **fault** | **netint** | **tlb**}

Syntax Description

buffers	Displays buffer-allocation information.
eeprom	Displays the internal information.
fault	Displays fault information.
netint	Displays network-interrupt information.
tlb	Displays information about the TLB registers.

Command Default

This command has no default settings.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

These examples display the **show msfc** command output:

```
Router# show msfc buffers
Reg. set    Min    Max
  TX               640
 ABQ        640  16384
   0          0     40
   1       6715   8192
   2          0      0
   3          0      0
   4          0      0
   5          0      0
   6          0      0
   7          0      0
Threshold = 8192
Vlan  Sel  Min  Max  Cnt  Rsvd
1016    1 6715 8192    0     0
Router#
Router# show msfc eeprom
RSFC CPU IDPROM:
IDPROM image:
  (FRU is 'Cat6k MSFC 2 daughterboard')
IDPROM image block #0:
  hexadecimal contents of block:
```

```
  00: AB AB 01 90 13 22 01 00 00 02 60 03 00 EA 43 69    ....."....`...Ci
  10: 73 63 6F 20 53 79 73 74 65 6D 73 00 00 00 00 00    sco Systems.....
  20: 00 00 57 53 2D 46 36 4B 2D 4D 53 46 43 32 00 00    ..WS-F6K-MSFC2..
  30: 00 00 00 00 00 00 53 41 44 30 36 32 31 30 30 36    ......SAD0621006
  40: 37 00 00 00 00 00 00 00 00 00 37 33 2D 37 32 33    7.........73-723
  50: 37 2D 30 33 00 00 00 00 00 00 41 30 00 00 00 00    7-03......A0....
  60: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
  70: 00 00 00 02 00 03 00 00 00 00 00 09 00 05 00 01    ................
  80: 00 03 00 01 00 01 00 02 00 EA FF DF 00 00 00 00    ................
  block-signature = 0xABAB, block-version = 1,
  block-length = 144, block-checksum = 4898
  *** common-block ***
  IDPROM capacity (bytes) = 256  IDPROM block-count = 2
  FRU type = (0x6003,234)
  OEM String = 'Cisco Systems'
  Product Number = 'WS-F6K-MSFC2'
  Serial Number = 'SAD06210067'
  Manufacturing Assembly Number = '73-7237-03'
  Manufacturing Assembly Revision = 'A0'
  Hardware Revision = 2.3
  Manufacturing bits = 0x0  Engineering bits = 0x0
  SNMP OID = 9.5.1.3.1.1.2.234
  Power Consumption = -33 centiamperes    RMA failure code = 0-0-0-0
  *** end of common block ***
IDPROM image block #1:
  hexadecimal contents of block:
  00: 60 03 01 62 0A C2 00 00 00 00 00 00 00 00 00 00    `..b............
  10: 00 00 00 00 00 01 00 23 00 08 7C A4 CE 80 00 40    .......#..|....@
  20: 01 01 00 01 00 00 00 00 00 00 00 00 00 00 00 00    ................
  30: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
  40: 14 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
  50: 10 00 4B 3C 41 32 80 80 80 80 80 80 80 80 80 80    ..K<A2..........
  60: 80 80                                              ..
  block-signature = 0x6003, block-version = 1,
  block-length = 98, block-checksum = 2754
  *** linecard specific block ***
  feature-bits =   00000000 00000000
  hardware-changes-bits =   00000000 00000001
  card index = 35
  mac base = 0008.7CA4.CE80
  mac_len = 64
  num_processors = 1
  epld_num = 1
  epld_versions = 0001 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 00
00 0000 0000
  port numbers:
    pair #0: type=14, count=01
    pair #1: type=00, count=00
    pair #2: type=00, count=00
    pair #3: type=00, count=00
    pair #4: type=00, count=00
    pair #5: type=00, count=00
    pair #6: type=00, count=00
    pair #7: type=00, count=00
  sram_size = 4096
  sensor_thresholds =
    sensor #0: critical = 75 oC, warning = 60 oC
    sensor #1: critical = 65 oC, warning = 50 oC
    sensor #2: critical = -128 oC (sensor not present), warning = -128 oC (senso
r not present)
    sensor #3: critical = -128 oC (sensor not present), warning = -128 oC (senso
r not present)
    sensor #4: critical = -128 oC (sensor not present), warning = -128 oC (senso
r not present)
```

```
    sensor #5: critical = -128 oC (sensor not present), warning = -128 oC (senso
r not present)
    sensor #6: critical = -128 oC (sensor not present), warning = -128 oC (senso
r not present)
    sensor #7: critical = -128 oC (sensor not present), warning = -128 oC (senso
r not present)
  *** end of linecard specific block ***
End of IDPROM image
Router#
Router# show msfc fault
 Reg. set    Min    Max
  TX               640
 ABQ        640  16384
   0          0     40
   1       6715   8192
   2          0      0
   3          0      0
   4          0      0
   5          0      0
   6          0      0
   7          0      0
Threshold = 8192
Vlan  Sel  Min  Max  Cnt  Rsvd
1016    1 6715 8192    0     0
Router#
Router# show msfc netint
Network IO Interrupt Throttling:
 throttle count=0, timer count=0
 active=0, configured=1
 netint usec=3999, netint mask usec=400
Router#
Router# show msfc tlb
Mistral revision 3
TLB entries : 37
Virt Address range      Phy Address range      Attributes
0x10000000:0x1001FFFF   0x010000000:0x01001FFFF   CacheMode=2, RW, Valid
0x10020000:0x1003FFFF   0x010020000:0x01003FFFF   CacheMode=2, RW, Valid
0x10040000:0x1005FFFF   0x010040000:0x01005FFFF   CacheMode=2, RW, Valid
0x10060000:0x1007FFFF   0x010060000:0x01007FFFF   CacheMode=2, RW, Valid
0x10080000:0x10087FFF   0x010080000:0x010087FFF   CacheMode=2, RW, Valid
0x10088000:0x1008FFFF   0x010088000:0x01008FFFF   CacheMode=2, RW, Valid
0x18000000:0x1801FFFF   0x010000000:0x01001FFFF   CacheMode=0, RW, Valid
0x19000000:0x1901FFFF   0x010000000:0x01001FFFF   CacheMode=7, RW, Valid
0x1E000000:0x1E1FFFFF   0x01E000000:0x01E1FFFFF   CacheMode=2, RW, Valid
0x1E880000:0x1E881FFF   0x01E880000:0x01E881FFF   CacheMode=2, RW, Valid
0x1FC00000:0x1FC7FFFF   0x01FC00000:0x01FC7FFFF   CacheMode=2, RO, Valid
0x30000000:0x3001FFFF   0x070000000:0x07001FFFF   CacheMode=2, RW, Valid
0x40000000:0x407FFFFF   0x000000000:0x0007FFFFF   CacheMode=3, RO, Valid
0x40800000:0x40FFFFFF   0x000800000:0x000FFFFFF   CacheMode=3, RO, Valid
0x41000000:0x417FFFFF   0x001000000:0x0017FFFFF   CacheMode=3, RO, Valid
0x41800000:0x419FFFFF   0x001800000:0x0019FFFFF   CacheMode=3, RO, Valid
0x41A00000:0x41A7FFFF   0x001A00000:0x001A7FFFF   CacheMode=3, RO, Valid
0x41A80000:0x41A9FFFF   0x001A80000:0x001A9FFFF   CacheMode=3, RO, Valid
0x41AA0000:0x41ABFFFF   0x001AA0000:0x001ABFFFF   CacheMode=3, RO, Valid
0x41AC0000:0x41AC7FFF   0x001AC0000:0x001AC7FFF   CacheMode=3, RO, Valid
0x41AC8000:0x41ACFFFF   0x001AC8000:0x001ACFFFF   CacheMode=3, RO, Valid
0x41AD0000:0x41AD7FFF   0x001AD0000:0x001AD7FFF   CacheMode=3, RO, Valid
0x41AD8000:0x41AD9FFF   0x001AD8000:0x001AD9FFF   CacheMode=3, RO, Valid
0x41ADA000:0x41ADBFFF   0x001ADA000:0x001ADBFFF   CacheMode=3, RW, Valid
0x41ADC000:0x41ADDFFF   0x001ADC000:0x001ADDFFF   CacheMode=3, RW, Valid
0x41ADE000:0x41ADFFFF   0x001ADE000:0x001ADFFFF   CacheMode=3, RW, Valid
0x41AE0000:0x41AFFFFF   0x001AE0000:0x001AFFFFF   CacheMode=3, RW, Valid
0x41B00000:0x41B7FFFF   0x001B00000:0x001B7FFFF   CacheMode=3, RW, Valid
0x41B80000:0x41BFFFFF   0x001B80000:0x001BFFFFF   CacheMode=3, RW, Valid
```

```
0x41C00000:0x41DFFFFF   0x001C00000:0x001DFFFFF   CacheMode=3, RW, Valid
0x41E00000:0x41FFFFFF   0x001E00000:0x001FFFFFF   CacheMode=3, RW, Valid
0x42000000:0x43FFFFFF   0x002000000:0x003FFFFFF   CacheMode=3, RW, Valid
0x44000000:0x45FFFFFF   0x004000000:0x005FFFFFF   CacheMode=3, RW, Valid
0x46000000:0x47FFFFFF   0x006000000:0x007FFFFFF   CacheMode=3, RW, Valid
0x06E00000:0x06FFFFFF   0x006E00000:0x006FFFFFF   CacheMode=2, RW, Valid
0x07000000:0x077FFFFF   0x007000000:0x0077FFFFF   CacheMode=2, RW, Valid
0x07800000:0x07FFFFFF   0x007800000:0x007FFFFFF   CacheMode=2, RW, Valid
Router#
```

Related Commands

Command	Description
show environment alarm	Displays the information about the environmental alarm.
show fm summary	Displays a summary of FM Information.
show environment status	Displays the information about the operational FRU status.

show network-clocks

To display the current configured and active network clock sources, use the**shownetwork-clocks** command in privileged EXEC mode.

show network-clocks

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRD1	This command was introduced to display BITS clock information for the 7600-ES+ITU-2TG and 7600-ES+ITU-4TG.

Usage Guidelines

On the Cisco MC3810, this command applies to Voice over Frame Relay, Voice over ATM, and Voice over HDLC. The Cisco MC3810 has a background task that verifies whether a valid clocking configuration exists every 120 seconds. If this task detects an error, you will be reminded every 120 seconds until the error is corrected. A clocking configuration error may be generated for various reasons. Using the **shownetwork-clocks** command, you can display the clocking configuration status.

On the Cisco 7600 series routers, this command applies to the following:

- The clock source from the POS SPAs on the SIP-200 and the SIP-400.
- The 24-Port Channelized T1/E1 ATM CEoP SPA and the 1-Port Channelized OC-3 STM1 ATM CEoP SPA on the SIP-400.
- The 7600-ES+ITU-2TG and 7600-ES+ITU-4TG line cards.

Examples

The following is sample output from the **shownetwork-clocks** EXEC command:

```
Router# show network-clocks
Priority 1 clock source: ATM3/0/0
Priority 2 clock source: System clock
Priority 3 clock source: System clock
Priority 4 clock source: System clock
Current clock source:ATM3/0/0, priority:1
```

The following is sample output from the **shownetwork-clocks** command on the Cisco MC3810:

```
Router# show network-clocks
Priority 1 clock source(inactive config): T1 0
Priority 1 clock source(active config) : T1 0
```

```
Clock switch delay: 10
Clock restore delay: 10
T1 0 is clocking system bus for 9319 seconds.
Run Priority Queue: controller0
```

In this display, inactive configuration is the new configuration that has been established. Active configuration is the run-time configuration. Should an error be made in the new configuration, the inactive and active configurations will be different. In the previous example, the clock priority configuration is valid, and the system is being clocked as indicated.

The following is another sample output from the **shownetwork-clocks** command:

```
Router# show network-clocks
Priority 1 clock source(inactive config) : T1 0
Priority 2 clock source(inactive config) : T1 1
Priority 1 clock source(active config) : T1 0
Clock switch delay: 10
Clock restore delay: 10
T1 0 is clocking system bus for 9319 seconds.
Run Priority Queue: controller0
```

In this display, the new clocking configuration has an error for controller T1 1. This is indicated by checking differences between the last valid configuration (active) and the new proposed configuration (inactive). The error may result from hardware (the system controller board or MFT) unable to support this mode, or controller T1 1 is currently configured as “clock source internal.”

Since the active and inactive configurations are different, the system will periodically display the warning message about the wrong configuration.

The following is another sample output from the **shownetwork-clocks** command for the 7600-ES+ITU-2TG or 7600-ES+ITU-4TG:

```
Router# show network-clocks
 Active source = Slot 1 BITS 0
 Active source backplane reference line = Primary Backplane Clock
 Standby source = Slot 9
 Standby source backplane reference line = Secondary Backplane Clock
(Standby source not driving backplane clock currently)
 All Network Clock Configuration
---------------------------------
 Priority  Clock Source            State                       Reason
 1         POS3/0/1                Valid but not present
 2         Slot 1 BITS 0           Valid
 3         Slot 9                  Valid
 Current operating mode is Revertive
 Current OOR Switchover mode is Switchover
There are no slots disabled from participating in network clocking
 BITS Port Configuration
-------------------------
 Slot    Port    Signal Type/Mode        Line Build-Out Select
```

1 0 T1 ESF DSX-1 (533 to 655 feet)

Related Commands

Command	Description
clock source	Specifies the interface clock source type.
network-clock	Configures BITS port signaling types.

Command	Description
network-clock select	Selects a source of network clock.
network-clock-select (ATM)	Establishes the sources and priorities of the requisite clocking signals for an ATM-CES port adapter.
show platform hardware network-clocks	Displays network clocks for an ES+ line card.

show pagp

To display port-channel information, use the **show pagp** command in user EXEC or privileged EXEC mode.

show pagp [*group-number*] {**counters** | **internal** | **neighbor** | **pgroup**}

Syntax Description

group-number	(Optional) Channel-group number; valid values are a maximum of 64 values from 1 to 282.
counters	Displays the traffic information.
internal	Displays the internal information.
neighbor	Displays the neighbor information.
pgroup	Displays the active port channels.

Command Default

This command has no default settings.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You can enter any **show pagp** command to display the active port-channel information. To display the nonactive information, enter the **show pagp** command with a group.

The **port-channel** *number*values from 257 to 282 are supported on the CSM and the FWSM only.

Examples

This example shows how to display information about the PAgP counters:

```
Router#
show pagp
 counters
           Information        Flush
Port       Sent   Recv      Sent   Recv
--------------------------------------
Channel group: 1
  Fa5/4    2660   2452      0      0
  Fa5/5    2676   2453      0      0
Channel group: 2
  Fa5/6    289    261       0      0
  Fa5/7    290    261       0      0
Channel group: 1023
  Fa5/9    0      0         0      0
Channel group: 1024
  Fa5/8    0      0         0      0
Router#
```

This example shows how to display internal PAgP information:

```
Router# show pagp
 1 internal
Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.
Timers: H - Hello timer is running.        Q - Quit timer is running.
        S - Switching timer is running.    I - Interface timer is running.
Channel group 1
                                Hello    Partner  PAgP     Learning
Port      Flags State   Timers  Interval Count   Priority  Method
Fa5/4     SC    U6/S7           30s      1        128      Any
Fa5/5     SC    U6/S7           30s      1        128      Any
Router#
```

This example shows how to display PAgP-neighbor information for all neighbors:

```
Router# show pagp
 neighbor
Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.        P - Device learns on physical port.
Channel group 1 neighbors
          Partner              Partner          Partner         Partner Group
Port      Name                 Device ID        Port       Age  Flags   Cap.
Fa5/4     JAB031301            0050.0f10.230c   2/45         2s SAC     2D
Fa5/5     JAB031301            0050.0f10.230c   2/46        27s SAC     2D
Channel group 2 neighbors
          Partner              Partner          Partner         Partner Group
Port      Name                 Device ID        Port       Age  Flags   Cap.
Fa5/6     JAB031301            0050.0f10.230c   2/47        10s SAC     2F
Fa5/7     JAB031301            0050.0f10.230c   2/48        11s SAC     2F
Channel group 1023 neighbors
          Partner              Partner          Partner         Partner Group
Port      Name                 Device ID        Port       Age  Flags   Cap.
Channel group 1024 neighbors
          Partner              Partner          Partner         Partner Group
Port      Name                 Device ID        Port       Age  Flags   Cap.
Router#
```

Related Commands

Command	Description
pagp learn-method	Learns the input interface of the incoming packets.
pagp port-priority	Selects a port in hot standby mode.

show pas caim

To show debug information about the data compression Advanced Interface Module (CAIM) daughter card, use the **showpascaim**command in user EXEC or privileged EXEC mode.

show pas caim {**rings** | **dma** | **coprocessor** | **stats** | **cnxt_table** | **page_table**} *element-number*

Syntax Description

rings *element-number*	Displays current content of the Direct Memory Access (DMA) ring buffer.
dma *element-number*	Displays registers of the Jupiter DMA controller.
coprocessor *element-number*	Displays registers of the Hifn 9711 compression coprocessor.
stats *element-number*	Displays statistics that describes operation of the data compression Advanced Interface Module (AIM).
cnxt_table *element-number*	Displays the context of the specific data compression AIM element.
page_table *element-number*	Displays the page table for each CAIM element.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.0(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command displays performance statistics that describe the operation of the CAIM. This command is primarily intended for engineering debug, but it can also be useful to Cisco support personnel and to Cisco customers in troubleshooting network problems. The table below lists the output values for this command.

Table 177: show pas caim Output Values and Descriptions

Value	Description
uncomp paks in	Number of packets containing uncompressed data input to the CAIM for compression.
comp paks out	Number of packets containing uncompressed data that were successfully compressed.
comp paks in	Number of packets containing compressed data input to the CAIM for compression.
uncomp paks out	Number of packets containing compressed data that were successfully decompressed.

Value	Description
uncomp bytes in / comp bytes out	Summarizes the compression performance of the CAIM. The “uncomp bytes in” statistic gives the total number of uncompressed bytes submitted to the CAIM for compression. The “Comp bytes out” statistic gives the resulting number of compressed bytes output by the CAIM. If one forms the ratio of “uncomp bytes in” to “comp bytes out”, one obtains the average compression ratio achieved by the CAIM.
comp bytes in / uncomp bytes out	Summarizes the decompression performance of the CAIM. The “comp bytes in” statistic gives the total number of compressed bytes submitted to the CAIM for decompression. The “uncomp bytes out” statistic gives the resulting number of uncompressed bytes output by the CAIM. The average decompression ratio achieved can be computed as the ratio of “uncomp bytes out” to “comp bytes in”. Note that each packet submitted for compression or decompression has a small header at the front which is always clear data and hence never compressed nor decompressed. The “comp bytes in / uncomp bytes out” and “uncomp bytes in / comp bytes out” statistics do not include this header.
uncomp paks/sec in	A time average of the number of packets per second containing uncompressed data submitted as input to the CAIM for compression. It is computed as the ratio of the “uncomp paks in” statistic to the “seconds since last clear” statistic.
comp paks/sec out	A time average of the number of packets per second containing uncompressed data which were successfully compressed by the CAIM. It is computed as the ratio of the “comp paks out” statistic to the “seconds since last clear” compressed by the CAIM. It is computed as the ratio of the “comp paks out” statistic to the “seconds since last clear” statistic.
comp paks/sec in	A time average of the number of packets per second containing compressed data submitted as input to the CAIM for decompression. It is computed as the ratio of the “comp paks in” statistic to the “seconds since last clear” statistic.
uncomp paks/sec out	A time average of the number of packets per second containing compressed data which were successfully decompressed by the CAIM. It is computed as the ratio of the “uncomp paks out” statistic to the “seconds since last clear” statistic. Note that the “uncomp paks/sec in”, “comp paks/sec out”, “comp paks/sec in”, and “uncomp paks/sec out” statistics are averages over the entire time since the last “clear count” command was issued. This means that as time progresses, these statistics become averages over an ever larger time interval. As time progresses, these statistics become ever less sensitive to current prevailing conditions. Note also that the “uncomp paks in”, “comp paks out”, “comp paks in”, and “uncomp paks out” statistics are 32-bit counters and can roll over from 0xffff ffff to 0. When they do so, the “uncomp paks/sec in”, “comp paks/sec out”, “comp paks/sec in”, and “uncomp paks/sec out” statistics can be rendered meaningless. It is therefore recommend that one issue a “clear count” command before sampling these statistics.
uncomp bits/sec in	A time average of the number of bits per second of uncompressed data which were submitted to the CAIM for compression. It is computed as the ratio of the “uncomp bytes in” statistic, times 8, to the “seconds since last clear” statistic.

Value	Description
comp bits/sec out	A time average of the number of bits per second of uncompressed data which were successfully compressed by the CAIM. It is computed as the ratio of the "comp bytes out" statistic, times 8, to the "seconds since last clear" statistic.
comp bits/sec in	A time average of the number of bits per second of compressed data which were submitted to the CAIM for decompression. It is computed as the ratio of the "comp bytes in" statistic, times 8, to the "seconds since last clear" statistic.
uncomp bits/sec out	A time average of the number of bits per second of compressed data which were successfully decompressed by the CAIM. It is computed as the ratio of the "uncomp bytes in" statistic, times 8, to the "seconds since last clear" statistic. Note again that these "bits/sec" statistics are time averages over the "seconds since last clear" statistics, and therefore become less and less sensitive to current conditions as time progresses. Also, these "bits/sec" statistics are computed from 32-bit counters, and when the counters roll over from the maximum 32-bit value to 0, the "bits/sec" statistics become inaccurate. It is again recommended that one issue the "clear count" command before sampling the "bits/sec" statistics.
The remaining statistics summarize operational state and error conditions encountered by the CAIM, and have the following interpretations:	
holdq	Gives the number of packets occupying the "hold queue" of the CAIM. The hold queue is a holding area, or "overflow" area, for packets to be processed by the CAIM. Normally, the CAIM is fast enough that no overflow into the hold queue occurs, and so normally this statistic should show zero.
hw_enable	Flag indicating if the CAIM is disabled or not. Zero implies disabled; one implies enabled. The CAIM can become disabled if certain fatal hardware error conditions are detected. It can be reenabled by issuing the **clearaim***element-number* command.
src_limited	Flag indicating if the CAIM is in "source limited" mode. In source limited mode, the CAIM can only process a single command at a time. In non source limited mode, the CAIM can process several commands at a time using a pipeline built into the 9711 coprocessor. Note that the normal mode of operation is "non-source limited", and there is no command to place the CAIM in "source limited" mode. Hence, this statistic should always read zero.
num cnxts	Gives the number of "contexts" which are currently open on the CAIM. Each interface configured for compression opens two contexts, one for each direction of data transfer.
no data	Counts the number of times in which the CAIM performed either a compress or decompression operation, and the output data length was reported with a length of zero. In normal operation, this statistic should always read zero. A nonzero value is an indication of a malfunctioning CAIM.

Value	Description
drops	Counts the total number of times in which the CAIM was forced to drop a packet it was asked to compress or decompress. This can happen for a number of reasons, and the remaining statistics summarize these reasons. This statistic indicates that the CAIM is being overloaded with requests for compression/decompression.
nobuffers	Counts the total number of times the CAIM needed to allocate memory for buffers but could not obtain memory. The CAIM allocates memory for buffers for holding the results of compression or decompression operations. In normal operation, there is plenty of memory available for holding CAIM results. This statistic, if nonzero, indicates that there is a significant backup in memory, or perhaps a memory leak.
enc adj errs	Each packet compressed or decompressed involves an adjustment of the encapsulation of the packet between the LZS-DCP, FRF9, or MPPC encapsulation used to transport compressed packets to the standard encapsulation used to transport clear data. This statistic counts the number of times this encapsulation adjustment failed. In normal operation, this statistic should be zero. A nonzero value indicates that we are short in a specific memory resource referred to as “paktypes”, and that packets are being dropped because of this shortage.
fallbacks	Number of times the data compression AIM card could not use its pre-allocated buffers to store compression results and had to “fallback” to using a common buffer pool.
no replace	Each time a compression or decompression operation is completed and the resultant data fill up a buffer, the CAIM software allocates a new buffer to replace the buffer filled. If no buffers are available, then the packet involved in this operation is dropped and the old buffer reused. This statistic thus represents the number of times such an allocation failure occurred. In normal operation there is plenty of memory available for these buffers. A nonzero value for this statistic is thus a serious indication of a memory leak or other backup in buffer usage somewhere in the system.
num seq errs	This statistic is incremented when the CAIM produces results in a different order than that in which the requests were submitted. Packets involved in such errors are dropped. A nonzero value in this statistic indicates a serious malfunction in the CAIM.
num desc errs	Incremented when the CAIM reports error in a compression or decompression operation. Such errors are most likely bus errors, and they indicate a serious malfunction in the CAIM.
cmds complete	Reports the number of compression/decompression commands completed. This statistic should steadily increase in normal operation (assuming that the CAIM is continuously being asked to perform compression or decompression). If this statistic is not steadily increasing or decreasing when a steady stream of compression/decompression is expected, this is an indication of a malfunctioning CAIM.
bad reqs	Reports the number of compression/decompression requests that the CAIM software determined it could not possibly handle. This occurs only if a severely scattered packet (with more than 64 “particles”, or separate buffers of data) is handed to the CAIM to compress or decompress. This statistic should not increment during normal operation. A nonzero value indicates a software bug.

Value	Description
dead cntxts	Number of times a packet was successfully compressed or decompressed, only to find that the software "context", or stream sourcing the packet, was no longer around. In such a case the packet is dropped. This statistic can be incremented at times when a serial interface is administratively disabled. If the timing is right, the CAIM may be right in the middle of operating on a packet from that interface when the disable takes effect. When the CAIM operation completes, it finds that the interface has been disabled and all "compression contexts" pertaining to that interface have been deleted. Another situation in which this can occur is when a Frame Relay DLC goes down. This is a normal and tolerable. If this statistic is incrementing when no such situations exist, it is an indication of a software bug.
no paks	If a packet to be compressed or decompressed overflows into the hold queue, then it must undergo an operation called "reparenting". This involves the allocation of a "paktype" structure for the packet. If no paktype structures are available, then the packet is dropped and this statistic is incremented. A nonzero value of this statistic indicates that the CAIM is being overtaxed, that is, it is being asked to compress/decompress at a rate exceeding its capabilities.
enq errors	Closely related to the "no paks" statistic. The hold queue for the CAIM is limited in length, and if the hold queue grows to this length, no further packets may be placed on it. A nonzero value of this statistic therefore also indicates that the CAIM is being overtaxed.
rx pkt drops	Contains the total number of packets dropped because of "no paks" or "enq errors", which were destined to be decompressed.
tx pkt drops	Contains the total number of packets dropped because of "no paks" or "enq errors", which were destined to be compressed
dequeues	Indicates the total number of packets which were removed from the CAIM hold queue when the CAIM became available for servicing its hold queue.
requeues	Indicates the total number of packets that were removed from the hold queue, only to find that the necessary CAIM resources were not available (it is not possible to determine whether CAIM resources are available until the packet is dequeued). Such packets are requeued onto the hold queue, with order in the queue preserved.
drops disabled	Indicates the total number of packets which were submitted for compression or decompression, but that were dropped because the CAIM was disabled.
clears	Indicates the number of times the CAIM was reset using the **clearaim***element-number*command.
# ints	Indicates the number of interrupts serviced by the CAIM software. This statistic should steadily increase (assuming that the CAIM workload is steady). If this statistic is not incremented when expected, it indicates a severe CAIM malfunction.

Value	Description
# purges	Indicates the total number of times the compression history for a session had to be purged. This statistic is incremented a couple of times at startup. Thereafter, any increase in this statistic is an indication that the other side of the serial link detected bad data or gaps in the compressed packets being passed to it, and hence signalled a request to purge compression history in order to get back in synchronization. This can indicate that the CAIM is being overtaxed or that the serial interface is overtaxed and being forced to drop output packets.
no cnxts	Indicates the total number of times a request was issued to open a context, but the CAIM could not support any more contexts. Recall that two contexts are required for each interface configured for compression.
bad algos	Indicates the total number of times a request was issued to open a context for a compression algorithm not supported by the CAIM. Recall that the CAIM supports the LZS and MPPC algorithms only.
no crams	Indicates the total number of times a request was issued to open a context but there was insufficient compression DRAM to open another context. The CAIM software is set up to run out of contexts before it runs out of compression DRAM, so this statistic should always be zero.
bad paks	Indicates the total number of times a packet was submitted for compression or decompression to the CAIM, but the packet had an invalid size.
# opens	Indicates the total number of times a context was opened.
# closes	Indicates the total number of times a context was closed.
# hangs	Indicates the total number of times a CAIM appeared hung up, necessitating a clear of the CAIM.

Examples

The **showpascaimrings***element-number* command displays the current state of the DMA ring buffers maintained by the CAIM software. These rings feed the CAIM with data and commands. It is intended for an engineering debug of the compression AIM. It produces the following output:

```
Router# show pas caim rings 0
CAIM Command Ring: 0x01A2BC00  Stack: 0x01A2BE40  Shadow: 0x80F88BAC
 Head: 0021  Tail: 0021  Count: 0000
CAIM Source Ring:  0x01A2C900  Shadow: 0x80F88BAC
 Head: 0021  Tail: 0021  Num: 0000
CAIM Results Ring: 0x01A2C280  Stack: 0x01A2C4C0
 Head=021  Tail=021
CAIM Dest Ring:    0x01A2CB40  Shadow: 0x80F892D8  Head=021  Tail=000
  Desc: 0x01A2CBE8  flags: 0x8000060C  dptr: 0x019E7EB8  part: 0x80F84BE0
  Desc: 0x01A2CBF0  flags: 0x8000060C  dptr: 0x019FC63C  part: 0x80F85240
.
.
.
```

The table below describes the significant fields shown in the display.

Table 178: show pas caim rings Field Descriptions

Field	Description
CAIM Command Ring	Feeds commands to the CAIM.
command ring address	Address of the command ring.
Command Ring Stack	Ring that feeds additional commands to the CAIM.
command ring stack address	Address of the command ring stack.
Command Ring Shadow	Software ring that stores additional information about each command.
command ring shadow address	Address of the command ring shadow.
Command Ring Head	Index into the Source Ring, specifying where the next entry will be extracted from.
Command Ring Tail	Index into the Source Ring, specifying where the next entry will be inserted.
CAIM Source Ring	Feeds information about input data to the CAIM.
source ring address	Address of the source ring.
Source Ring Shadow	Ring that contains additional information about each source buffer.
source ring shadow address	Address of the source ring shadow.
Source Ring Head	Specifies where the next entry will be extracted from.
Source Ring Tail	Specifies where the next entry will be inserted.
CAIM Results Ring	Receives information about each CAIM command as it is completed.
results ring address	Address of the results ring.
Results Ring Stack	Ring that receives additional information about each completed command.
results ring stack address	Address of the results ring stack.
Results Ring Head	Specifies where the next entry will be extracted from.
Results Ring Tail	Specifies where the next entry will be inserted.
CAIM Dest Ring	Holds information about the buffers available to the CAIM for output data.
dest ring address	Address of the dest ring.
Dest Ring Shadow	Ring that holds additional information about each output buffer.

Field	Description
dest ring shadow address	Address of the dest ring shadow.
Dest Ring Head	Index into the Source Ring, specifying where the next entry will be extracted from.
Dest Ring Tail	Index into the Source Ring, specifying where the next entry will be inserted.
The remaining fields describe each output data buffer.	
dest	Address of a so-called descriptor, used by the Jupiter DMA engine.
flags	Contains flags describing attributes of the buffer.
dptr	Displays the actual address of the output buffer.
part	Displays the address of the corresponding particle type structure, a software-defined structure that describes a buffer when it is a component of a network data buffer.

The **show pas caim dma** *element-number*command displays the registers of the Jupiter DMA Controller. These registers control the operation of the Jupiter DMA Controller. This command is intended for Engineering debug of the CAIM. You can find detailed descriptions of the various fields in the Jupiter DMA Controller specification. It produces the following output:

```
Router# show pas caim dma 0
Jupiter DMA Controller Registers: (0x40200000
        Cmd Ring: 0x01A2BCA8  Src Ring: 0x01A2C9A8
        Res Ring: 0x01A2C328  Dst Ring: 0x01A2CBE8
        Status/Cntl: present: 0x80808084  last int: 0x80808084
        Inten: 0x10100000  config: 0x00100003
        Num DMA ints: 143330469
```

The show pas caim compressor element-number command displays the registers of the Hifn 9711 compression coprocessor. These registers control the operation of the Hifn 9711 part. This command is intended for engineering to debug the CAIM. Detailed descriptions of the various fields may be found in the Hifn 9711 data book. It produces the following output:

```
Router# show pas caim compressor 0
Hifn9711 Data Compression Coprocessor Registers (0x40201000):
        Config: 0x000051D4  Inten: 0x00000E00
        Status: 0x00004000  FIFO status: 0x00004000
        FIFO config: 0x00000101
```

The table below describes the fields shown in the preceding display.

Table 179: show pas caim compressor Field Descriptions

Field	Description
Hifn9711 Data Compression Coprocessor Registers	Controls the operation of the Hifn 9711 part.

Field	Description
registers address	Address of the registers in the address space of the processor.
Config	Displays the current contents of the 9711 configuration register.
Inten	Displays the contents of the 9711 interrupt enable register.
Status	Displays the contents of the 9711 status register.
FIFO status	Contents of the 9711 FIFO Status register.
FIFO config	Contents of the 9711 FIFO Config register.

The show pas caim cnxt_table element-number command displays the context table for the specified CAIM element. The context table is a table of information concerning each compression context. It produces the following output:

```
Router# show pas caim cnxt_table 0
CAIM0 Context Table
Context: 0x8104F320  Type: Compr   Algo: Stac
    Hdrlen: 0006  History: 0x0000
    Callback: 0x8011D68C  Shutdown: x8011EBE4  Purge: N
    Comp_db: 0x81034BC0  idb: 0x81038084  ds: 0x8104E514
Context: 0x8104F340  Type: Decomp  Algo: Stac
    Hdrlen: 0002  History: 0x0000
    Callback: 0x8011E700  Shutdown: x8011EBE4  Purge: N
    Comp_db: 0x81034BC0  idb: 0x81038084  ds: 0x8104E514
```

The table below describes the fields shown in the preceding display.

Table 180: show pas caim cnxt_table Fields Descriptions

Field	Description
Context	Numeric internal reference for the compression context.
Type	Gives the type of context: • Compr--compression context • Decomp--decompression context
Algo	Gives the compression algorithm used: • Stac • Mppc
Hdrlen	Gives the number of bytes in the compression header for each compressed packet.
History	Gives the 16-KB page number in compression RAM for the context.
Callback	Gives an internal numeric reference for a control structures or procedure to facilitate debugging.
Shutdown	Gives an internal numeric reference for a control structures or procedure to facilitate debugging.

Field	Description
Comp_db	Gives an internal numeric reference for a control structures or procedure to facilitate debugging.
idb	Gives an internal numeric reference for a control structures or procedure to facilitate debugging.
idb	Gives an internal numeric reference for a control structures or procedure to facilitate debugging.
Purge	Indicates whether the compression context has been flagged to have its history purged.

The show pas caim page_table element-number command displays the page table for the selected CAIM element. The page table is a table of entries describing each page in compression RAM. It produces the following output:

```
Router# show pas caim page_table 0
CAIM0 Page Table
    Page  0x0000 Comp cnxt: 8104F320  Decmp cnxt: 8104F340  Algo: Stac
```

The table below describes the fields shown in the preceding display.

Table 181: show pas caim page_table Field Descriptions

Field	Description
Page	16 KB page number of the page.
Comp cnxt	Contains an internal numeric reference to the context structures using this page.
Decmp cnxt	Contains an internal numeric reference to the context structures using this page.
Algo	Gives the compression algorithm used: • Stac • Mppc

The following example shows statistics of an active data compression AIM session:

```
Router# show pas caim stats 0
CompressionAim0
    ds:0x80F56A44 idb:0x80F50DB8
        422074 uncomp paks in -->       422076 comp paks out
        422071 comp paks in   -->       422075 uncomp paks out
     633912308 uncomp bytes in-->     22791798 comp bytes out
      27433911 comp bytes in  -->    633911762 uncomp bytes out
           974 uncomp paks/sec in-->       974 comp paks/sec out
           974 comp paks/sec in  -->       974 uncomp paks/sec out
      11739116 uncomp bits/sec in-->    422070 comp bits/sec out
        508035 comp bits/sec in  -->  11739106 uncomp bits/sec out
    433 seconds since last clear
    holdq: 0  hw_enable: 1  src_limited: 0  num cnxts: 4
    no data: 0  drops: 0  nobuffers: 0  enc adj errs: 0  fallbacks: 0
    no Replace: 0  num seq errs: 0  num desc errs: 0  cmds complete: 844151
    Bad reqs: 0  Dead cnxts: 0  No Paks: 0  enq errs: 0
    rx pkt drops: 0  tx pkt drops: 0  dequeues: 0  requeues: 0
    drops disabled: 0  clears: 0  ints: 844314  purges: 0
    no cnxts: 0  bad algos: 0  no crams: 0  bad paks: 0
    # opens: 0  # closes: 0 # hangs: 0
```

Related Commands

Command	Description
show compress	Displays compression statistics.

show pas eswitch address

To display the Layer 2 learned addresses for an interface, use the **showpaseswitchaddress** command in user EXEC or privileged EXEC mode.

show pas eswitch address commandshow pas eswitch address [{**ethernet**|**fastethernet**}] [*slot*/*port*]

Syntax Description

ethernet | **fastethernet**	(Optional) Type of interface.
slot	(Optional) Slot number of the interface.
port	(Optional) Interface number.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
11.2P	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following sample output shows that the first PA-12E/2FE interface (listed below as port 0) in port adapter slot 3 has learned the Layer 2 address 00e0.f7a4.5100 for bridge group 30 (listed below as BG 30):

```
Router# show pas eswitch address fastethernet 3/0
U 00e0.f7a4.5100, AgeTs 56273 s, BG 30 (vLAN 0), Port 0
```

show pas i82543 interface

To display interface information that is specific to Fast Ethernet or Gigabit Ethernet port adapters with an Intel 82543 processor on Cisco 7200 series routers, use the **showpasi82543interface**command in privileged EXEC mode.

show pas i82543 interface {**fastethernet** | **gigabitethernet**} *slot/port* [{**multicast-table** | **receive-address** | **statistics**}]

Syntax Description

fastethernet	Displays i82543-specific information for Fast Ethernet interfaces.
gigabitethernet	Displays i82543-specific information for Gigabit Ethernet interfaces.
slot	Slot number.
/ *port*	Port number. The slash mark is required between the *slot* argument and the *port* argument.
multicast-table	(Optional) Displays i82543-specific multicast address table information. **Note** In Cisco IOS Release 12.2 S, this keyword is **MTA**.
receive-address	(Optional) Displays the contents of the receive address registers on the i82543 chip.
statistics	(Optional) Displays i82543-specific statistical information.

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
12.2(20)S	This command was introduced on Cisco 7200 series routers.
12.1(20)E	This command was integrated into Cisco IOS Release 12.1(20)E on Cisco 7200 series routers.
12.0(27)S	This command was integrated into Cisco IOS Release 12.0(27)S on Cisco 7200 series routers.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T on Cisco 7200 series routers.

Usage Guidelines

Use the **showpasi82543interface** command with the **statistics** keyword to determine what types of packets are being processed. Similar statistical information is displayed by the **showcontrollersfastethernet** and **showcontrollersgigabitethernet** commands.

Note We recommend that the **multicast-table** and **receive-address** keywords for this command be used only under the supervision of a Cisco engineer because of the cryptic output.

Examples

The following sample output shows the contents of the multicast address table present on the i82543 processor.

```
Router# show pas i82543 interface fastethernet 6/0 multicast-table
Multicast Table Entry #0 = 0x10000
Multicast Table Entry #1 = 0x1
Multicast Table Entry #84 = 0x8000
```

The following sample output shows the contents of the Receive Address High (RAH) and Receive Address Low (RAL) registers on the i82543 processor.

```
Router# show pas i82543 interface fastethernet 6/0 receive-address
#1 RAH 0x8000A8FC RAL 0x67B60900
#3 RAH 0x0003FFFF RAL 0xFF45F75B
#5 RAH 0x0003FFFF RAL 0xCBEE539A
#7 RAH 0x0003FFFF RAL 0x5ABDADEB
#9 RAH 0x0003FFFF RAL 0x365B5ACF
#11 RAH 0x0003FFFF RAL 0xB2D9B0CE
#13 RAH 0x0003FFFF RAL 0x12A91CF6
#15 RAH 0x0003FFFF RAL 0xEF4A3125
#17 RAH 0x0003FFFF RAL 0x1A07EB7D
#19 RAH 0x0003FFFF RAL 0xFF9B6EF8
#21 RAH 0x0003FFFF RAL 0xB7C2AFC9
#23 RAH 0x0003FFFF RAL 0x14F4FB0A
#25 RAH 0x0003FFFF RAL 0xC60D6706
#27 RAH 0x0003FFFF RAL 0x5E9DE230
#29 RAH 0x0003FFFF RAL 0x5FEF9FBE
#31 RAH 0x0003FFFF RAL 0xBBCCC57E
```

The following sample output shows packet statistics of the i82543 processor.

```
Router# show pas i82543 interface fastethernet 6/0 statistics
i82543 (Livengood) Statistics
  CRC error         0             Symbol error     0
  Missed Packets    0             Single Collision 0
  Excessive Coll    0             Multiple Coll    0
  Late Coll         0             Collision        0
  Defer             0             Receive Length   0
  Sequence Error    0             XON RX           0
  XON TX            0             XOFF RX          0
  XOFF TX           0             FC RX Unsupport  0
  Packet RX (64)    0             Packet RX (127)  0
  Packet RX (255)   0             Packet RX (511)  0
  Packet RX (1023)  0             Packet RX (1522) 0
  Good Packet RX    348           Broadcast RX     0
  Multicast RX      319           Good Packet TX   0
  Good Octets RX.H  0             Good Octets RX.L 0
  Good Octets TX.H  0             Good Octets TX.L 0
  RX No Buff        0             RX Undersize     0
  RX Fragment       0             RX Oversize      0
  RX Octets High    0             RX Octets Low    0
  TX Octets High    0             TX Octets Low    0
  TX Packet         0             RX Packet        348
  TX Broadcast      0             TX Multicast     0
  Packet TX (64)    0             Packet TX (127)  0
  Packet TX (255)   0             Packet TX (511)  0
  Packet TX (1023)  0             Packet TX (1522) 0
  TX Underruns      0             TX No CRS        0
  RX Error Count    0             RX DMA Underruns 0
  RX Carrier Ext    0
  TCP Segmentation  0             TCP Seg Failed   0
```

The table below describes significant fields shown in the display.

Table 182: ***show pas i82543 interface statistics*** *Field Descriptions*

Field	Description
CRC error	Cyclic redundancy checksum (CRC) generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data.
Symbol error	Number of symbol errors between reads.
Missed Packets	Indicates whether the software processes that handle the line protocol believe that the interface is usable (that is, whether keepalives are successful) or if it has been taken down by an administrator.
Single Collision	Number of times that a transmit operation encountered a single collision.
Excessive Coll	This counter is incremented after a transmit operation has encountered more than 16 collisions.
Multiple Coll	Number of times that a transmit operation encountered more than 1 collision, but less than 16 collisions.
Late Coll	Number of late collisions. A late collision happens when a collision occurs after transmitting the preamble. The most common cause of late collisions is Ethernet cable segments that are too long for the speed at which you are transmitting.
Collision	Number of messages transmitted because of an Ethernet collision. A packet that collides is counted only once in output packets.
Defer	Defer indicates that the chip had to defer while ready to transmit a frame because the carrier was asserted.
Receive Length	Number of receive length error events. A receive length error occurs if an incoming packet passes the filter criteria but is either oversized or undersized. Packets less than 64 bytes are undersized. Packets over 1522 bytes are oversized if LongPacketEnable (LPE) is 0. If LPE is 1, a packet is considered oversized if it exceeds 16,384 bytes.
Sequence Error	Number of sequence error events.
XON RX	Number of XON packets received.
XON TX	Number of XON packets transmitted.
XOFF RX	Number of XOFF packets received.
XOFF TX	Number of XOFF packets transmitted.
FC RX Unsupport	Number of unsupported flow control frames received.
Packet RX	Number of received packets of the following lengths in bytes: 64, 127, 255, 511, 1023, 1522.
Good Packet RX	Number of received packets without errors.

Field	Description
Broadcast RX	Number of broadcast packets received.
Multicast RX	Number of multicast packets received.
Good Packet TX	Number of transmitted packets without errors.
Good Octets	Number of good (without errors) octets received (RX) or transmitted (TX).
RX No Buff	Number of times that frames were received when there were no available buffers in host memory to store those frames. The packet will be received if there is space in FIFO memory.
RX Undersize	Number of received frames that passed through address filtering and were less than the minimum size of 64 bytes (from destination address through CRC, inclusively), but that contained a valid CRC.
RX Fragment	Number of received frames that passed through address filtering and were less than the minimum size of 64 bytes (from destination address through CRC, inclusively), but that contained a bad CRC.
RX Oversize	Number of received frames that passed through address filtering and were greater than the maximum size.
RX Octets	Total number of octets received.
TX Octets	Total number of octets transmitted.
TX Packet	Number of transmitted packets.
RX Packet	Number of received packets.
TX Broadcast	Number of broadcast packets transmitted.
TX Multicast	Number of multicast packets transmitted.
Packet TX	Number of transmitted packets of the following lengths in bytes: 64, 127, 255, 511, 1023, 1522.
TX Underruns	Number of times that the transmitter has been running faster than the router can handle. This may never be reported on some interfaces.
TX No CRS	Number of successful packet transmissions in which Carrier Sense (CRS) input from the physical layer was not asserted within one slot time of start of transmission.
RX Error Count	Number of receive packets in which RX_ER was asserted by the physical layer.
RX DMA Underruns	Number of receive direct memory access (DMA) underruns observed by the DMA.
RX Carrier Ext	Number of packets received in which the carrier extension error was signalled across the gigabit medium independent interface (GMII) interface.
TCP Segmentation	Number of TCP segmentation offload transmissions to the hardware.

Field	Description
TCP Seg Failed	Number of TCP segmentation offload transmissions to the hardware that failed to transmit all data in the TCP segmentation context payloads.

Related Commands

Commands	Description
show compress	Displays compression statistics.
show controllers fastethernet	Displays information about Fast Ethernet controllers.
show controllers gigabitethernet	Displays information about Gigabit Ethernet controllers.
show interfaces	Displays information about interfaces.

show pas isa controller

To show controller information that is specific to the Virtual Private Network (VPN) accelerator controller when an Integrated Services Adapter (ISA) is installed, use the **showpasisacontroller**EXEC command.

show pas isa controller

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **showpasisacontroller** command:

```
Router# show pas isa controller
Interface ISA5/1 :
Encryption Mode = IPSec
Addresses of Rings and instance structure:
High Priority Rings
   TX: 0x4B0E97C0 TX Shadow:0x62060E00
   RX: 0x4B0EB840 RX Pool:0x4B0EBC80 RX Pool Shadow:0x62068E58
Low Priority Rings
   TX: 0x4B0EA800 TX Shadow:0x62066E2C
   RX: 0x4B0EC0C0, RX Shadow:0x62069284
Instance Structure address:0x620603D8
Firmware write head/tail offset:0x4B0EC900
Firmware read  head/tail offset:0x3EA00000
```

Related Commands

Command	Description
show pas isa interface	Displays interface status information that is specific to the VPN accelerator card.

show pas isa interface

To display interface information that is specific to the Virtual Private Network (VPN) accelerator card when an Integrated Services Adapter (ISA) is installed, use the **showpasisainterface**command in privileged EXEC mode.

show pas isa interface

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **showpasisainterface** command:

```
Router# show pas isa interface
Interface ISA5/1 :
        Statistics of packets and bytes through this interface:
           2876894 packets in                   2910021 packets out
               420 paks/sec in                      415 paks/sec out
              2327 Kbits/sec in                    2408 Kbits/sec out
               632 commands out                     632 commands acknowledged
        low_pri_pkts_sent     1911    low_pri_pkts_rcvd:      1911
        invalid_sa:           260     invalid_flow:           33127
        invalid_dh:           0       ah_seq_failure:         0
        ah_spi_failure:       0       esp_auth_failure:       0
        esp_seq_failure:      0       esp_spi_failure:        0
        esp_protocol_absent:  0       ah_protocol_absent:     0
        bad_key_group:        0       no_shared_secret:       0
        no_skeyids:           0       pad_size_error:         0
        cmd_ring_full:        0       bulk_ring_full:         990
        bad_peer_pub_len:     0       authentication_failure: 0
        fallback:             1606642 no_particle:            0
        6922 seconds since last clear of counters
```

The table below describes the significant fields shown in the display.

Table 183: show pas isa interface Field Descriptions

Field	Description
packets in/out	Number of data packets received from, or sent to, the Integrated Service Adapter (ISA).

Field	Description
paks/sec in/out	Number of packets received in, or sent out, with the total number of seconds that the ISA is active.
Kbits/sec in/out	Number of kilobits (Kbits) received in, or sent out, with the total number of seconds that the ISA is active.
commands out	Number of commands going to the ISA. Examples of commands include setting up encryption sessions and retrieving statistics or status from the ISA.
commands acknowledged	Number of commands returning from the ISA. Examples of commands include setting up encryption sessions and retrieving statistics or status from the ISA.
low_pri_pkts_sent	This is a summary counter for number of Internet Key Exchange (IKE) and IPSec commands submitted to ISA.
low_pri_pkts_rcvd	This is a summary counter for number of IKE & IPSEC command responses received from ISA.
invalid_sa	Reference to an unusable security association key pair.
invalid_flow	An invalid packet using an IPSec key is received for encryption or decryption. Example: session has expired.
invalid_dh	Reference to an unusable Diffie-Hellman(DH) key pair.
ah_seq_failure	Unacceptably late Authentication Header (AH) header received.
ah_spi_failure	SPI specified in the AH header does not match the SPI associated with the IPSec AH key.
esp_auth_failure	Number of ESP packets received with authentication failures.
esp_seq_failure	Unacceptably late ESP packet received.
esp_spi_failure	SPI specified in the ESP header does not match the SPI associated with the IPSec ESP key.
esp_protocol_absent	Packet is missing expected ESP header.
ah_protocol_absent	Packet is missing expected AH header.
bad_key_group	Unsupported key group requested during a Diffie-Hellman generation.
no_shared_secret	Attempting to use a Diffie-Hellman shared secret that is not generated.
no_skeyids	Attempting to use a shared secret that is not generated.
pad_size_error	The length of the ESP padding is greater than the length of the entire packet.
cmd_ring_full	New IKE setup messages are not queued for processing until the previous queued requests are processed.

Field	Description
bulk_ring_full	New packets requiring IPSec functionality are not queued to the ISA until the ISA completes the processing of existing requests.
bad_peer_pub_len	Length of peer's DH public key does not match the length specified for the negotiated DH key group.
authentication_failure	Authentication failed.
fallback	The number of instances when the driver is successful in getting a replacement buffer from the global pool.
no_particle	The number of instances when the driver was unable to get a replacement buffer from the driver pool and the global (fallback) pool.

Related Commands

Command	Description
show pas isa controller	Displays controller status information that is specific to the VPN accelerator card.

show pas vam controller

To display controller information that is specific to the VPN Acceleration Module (VAM), use the **showpasvamcontroller** command in privileged EXEC mode.

show pas vam controller

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(9)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Examples

The following is sample output from the**showpasvamcontroller**command:

```
Router# show pas vam controller
Encryption Mode = IPSec
Addresses of Rings and instance structure:
Low Priority Queue:
    OMQ=0xF2CB2E0, OMQ Shadow = 0x630E6638, {1, 1, 0, 256}
    PKQ=0xF2CF320, PKQ Shadow = 0x630EBE64, {232, 232, 0, 256}
    ERQ=0xF2D3360, ERQ Shadow = 0x630F1690, {0, 0, 0, 256}
High Priority Rings:
   TX: 0x0F2D73A0 TX Shadow:0x630F6EBC, {6, 6, queued=0}
   RX: 0x7F2D93E0 {13, 0, 256}
   RX Pool:0x7F2DA420 RX Pool Shadow:0x630FCAE8, {6, 0, 255}
Instance Structure address:0x630E5898
Misc registers:
mini-omq=0xF2DB460, shdw=0x63102714
Group0=0x3D800000, Group1=0x3D801000
IndexReg = 0xDFFE700
Heartbeat info:<Addr, Value> = <0xF2DB520, 0x2A55A>
Running default HSP (addr=0x629D36AC, size=294268)
```

Related Commands

Command	Description
show pas vam interface	Displays interface status information specific to the VPN accelerator module.

show pas vam interface

To display interface information that is specific to the VPN Acceleration Module (VAM), use the **showpasvaminterface** command in privileged EXEC mode.

show pas vam interface

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(9)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

Enter the**showpasvaminterface** command to see if the VAM is currently processing crypto packets.

Examples

The following is sample output from the **showpasvaminterface** command:

```
Router# show pas vam interface
Interface VAM 2/1 :
        ds: 0x621CE0D8        idb:0x621C28DC
        Statistics of packets and bytes that through this interface:
              1110 packets in                  1110 packets out
            123387 bytes in                  100979 bytes out
                 0 paks/sec in                    0 paks/sec out
                 0 Kbits/sec in                   0 Kbits/sec out
              3507 commands out                3507 commands acknowledged
        ppq_full_err   : 0            ppq_rx_err       : 0
        cmdq_full_err  : 0            cmdq_rx_err      : 0
        no_buffer      : 0            fallback         : 0
        dst_overflow   : 0            nr_overflow      : 0
        sess_expired   : 0            pkt_fragmented   : 0
        out_of_mem     : 0            access_denied    : 0
        invalid_fc     : 0            invalid_param    : 0
        invalid_handle : 0            output_overrun   : 0
        input_underrun : 0            input_overrun    : 0
        key_invalid    : 0            packet_invalid   : 0
        decrypt_failed : 0            verify_failed    : 0
        attr_invalid   : 0            attr_val_invalid : 0
        attr_missing   : 0            obj_not_wrap     : 0
        bad_imp_hash   : 0            cant_fragment    : 0
        out_of_handles : 0            compr_cancelled  : 0
        rng_st_fail    : 0            other_errors     : 0
        3420 seconds since last clear of counters
```

The table below describes the significant fields shown in the display.

Table 184: show pas vam interface Field Descriptions

Field	Description
packets in/out	Number of data packets received from, or sent to, the VAM.
bytes in/out	Number of data bytes received from, or sent to, the VAM.
paks/sec in/out	Number of packets received in, or sent out, with the total number of seconds that the VAM is active.
Kbits/sec in/out	Number of kilobits (Kbits) received in, or sent out, with the total number of seconds that the VAM is active.
commands out	Number of commands going to the VAM. Examples of commands include setting up encryption sessions and retrieving statistics or status from the VAM.
commands acknowledged	Number of commands returning from the VAM. Examples of commands include setting up encryption sessions and retrieving statistics or status from the VAM.
ppq_full_err	Number of packets dropped because of a lack of space in the packet processing queues for the VAM. This usually means that input traffic has reached VAM maximum throughput possible.
ppq_rx_err	Summary counter for all errors related to packet processing.
cmdq_full_err	Number of commands dropped because of a lack of space in the command processing queues for the VAM. This error indicates that the input tunnel setup rate has reached the VAM maximum setup rate. The Internet Key Exchange (IKE) process retries the tunnel creation and deletion when commands are dropped by VAM.
cmdq_rx_err	Summary counter for all errors related to command processing (for example, IKE, or IPSec session creation or deletion).
no_buffer	Errors related to the VAM running out of buffers. May occur with large packets. Although VAM buffers cannot be tuned, try tuning buffers for other interfaces.
fallback	Internal VAM buffer pool is completely used up and VAM has to fallback to global buffer pool. This may cause minor performance impact, however, packets are still processed so this error can be ignored.
dst_overflow	Counter that is incremented when the VAM has completed an operation, but there is no available space into which to place the result.
nr_overflow	Counter that is incremented when the VAM has completed an operation, but there is no available space into which to place the result.
sess_expired	Counter that is incremented if the session used to encrypt or decrypt the packet has expired because of time or space limit.
pkt_fragmented	Counter that is incremented when the input packet has to be fragmented after encryption. This counter should always be 0 as fragmentation by VAM is disabled.
out_of_mem	Counter that is incremented when the VAM runs out of memory.

Field	Description
access_denied	Counter that is incremented when the VAM is requested to perform an operation on an object that can not be modified.
invalid_fc	Counter that is incremented when the VAM has received a request that is illegal for the specified object type.
invalid_param	Counter that is incremented when the VAM has received invalid parameters within a command.
invalid_handle	Counter that is incremented when the VAM receives a request for an operation to be performed on an object that does not exist.
output_overrun	Counter that is incremented when the space allocated for a response is not large enough to hold the result posted by the VAM.
input_underrun	Counter that is incremented when the VAM receives a packet for which it finds a premature end to the data, for example, a truncated packet.
input_overrun	Counter that is incremented when the VAM receives a buffer that is too large for the requested operation.
key_invalid	Counter that is incremented when the VAM receives a request for an operation on a key where the key is invalid or of the wrong type.
packet_invalid	Counter that is incremented when the VAM receives a packet whose body is badly formed.
decrypt_failed	Counter that is incremented when the VAM receives a packet that cannot be decrypted because the decrypted data was not properly formatted (for example, padding is wrong).
verify_failed	Counter that is incremented when the VAM receives a packet which could not be verified because the verification of a signature or authentication value failed.
attr_invalid	Counter that is incremented when the VAM receives a packet which specifies an attribute that is not correct for the specified object or operation.
attr_val_invalid	Counter that is incremented when the VAM encounters errors during packet or command processing. The packets or commands are dropped in such cases.
attr_missing	Counter that is incremented when the VAM receives an operation request for which the value of a required attribute is missing.
obj_not_wrap	Counter that is incremented when the VAM receives an operation request to retrieve an object that is hidden or unavailable for export beyond the FIPS boundary of the VPN Module.
bad_imp_hash	Counter that is incremented when the VAM sees a hash miscompare on unwrap.
cant_fragment	Counter that is incremented when the VAM determines a need to fragment a packet, but cannot fragment because the “don’t fragment” bit is set. This counter should always be zero because the fragmentation on the VAM is disabled.

Field	Description
out_of_handles	Counter that is incremented when the VAM has run out of available space for objects of the requested type.
comp_cancelled	Due to the operation of the compression algorithm, some data patterns cannot be compressed. Usually data that has already been compressed or data that does not have a sufficient number of repetitive patterns cannot be compressed and a compress operation would actually result in expansion of the data. There are certain known data patterns which do not compress. In these cases, the compression engine cancels the compression of the data and returns the original, uncompressed data without an IPPCP header. These counters are useful to determine if the content of the traffic on the network is actually benefiting from compression. If a large percentage of the network traffic is already compressed files, these counters may indicate that compression on these streams are not improving the performance of the network.
rng_st_fail	Counter that is incremented when the VAM detects a Random Number Generator self test failure.
pkt_replay_err	Counter that is incremented when a replay error is detected by the VAM.
other_errors	Counter that is incremented when the VAM encounters a packet or command error that is not listed in other error categories. An example could be if the packet IP header checksum is incorrect.

Related Commands

Command	Description
show pas vam controller	Displays controller status information that is specific to the VPN accelerator module.

show pas y88e8k interface

To display the y88e8k Port Adaptor Information (pas) message details of a Gigabit Ethernet interface, use the **showpasy88e8kinterface** command in User EXEC or privileged EXEC mode.

show pas y88e8k interface *type number* {**registers** | **rx_ring** | **statistics** | **tx_ring**}

Syntax Description

type	(Optional) Displays the interface type.
number	(Optional) Displays the interface number.
registers	Displays register values.
rx -ring	Displays the receive ring entries of the interface.
statistics	Displays the y88e8k chip statistics values.
tx -ring	Displays the transmit ring entries of the interface.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.4(22)T	This command was introduced in a release earlier than Cisco IOS Release 12.4(22)T.

Examples

The following is sample output from the **showpasy88e8kinterface** command:

```
Router# show pas y88e8k interface gigabit ethernet 1/0 rx-ring
Rx Ring:
 --------
  ring size = 128, particle size = 2048
  ring head = 0, tail = 127
  Ring entries:
     rxr       next_desc_addr   buf_ctrl   buf_addr_lo frame_sw  rxr_shadow   data_start
data_bytes
  0  0x642AE918  0x2DD9F020    0xC8550800 0x0DDA3180  0x00000000 0x64525440  0x2DDA3180  0
  1  0x642AE938  0x2DD9F040    0xC8550800 0x0DDA3A00  0x00000000 0x64525480  0x2DDA3A00  0
  2  0x642AE958  0x2DD9F060    0xC8550800 0x0DDA4280  0x00000000 0x645254C0  0x2DDA4280  0
  3  0x642AE978  0x2DD9F080    0xC8550800 0x0DDA4B00  0x00000000 0x64525500  0x2DDA4B00  0
  4  0x642AE998  0x2DD9F0A0    0xC8550800 0x0DDA5380  0x00000000 0x64525540  0x2DDA5380  0
  5  0x642AE9B8  0x2DD9F0C0    0xC8550800 0x0DDA5C00  0x00000000 0x64525580  0x2DDA5C00  0
  6  0x642AE9D8  0x2DD9F0E0    0xC8550800 0x0DDA6480  0x00000000 0x645255C0  0x2DDA6480  0
  7  0x642AE9F8  0x2DD9F100    0xC8550800 0x0DDA6D00  0x00000000 0x64525600  0x2DDA6D00  0
  8  0x642AEA18  0x2DD9F120    0xC8550800 0x0DDA7580  0x00000000 0x64525640  0x2DDA7580  0
  9  0x642AEA38  0x2DD9F140    0xC8550800 0x0DDA7E00  0x00000000 0x64525680  0x2DDA7E00  0
  10 0x642AEA58  0x2DD9F160    0xC8550800 0x0DDA8680  0x00000000 0x645256C0  0x2DDA8680  0
  11 0x642AEA78  0x2DD9F180    0xC8550800 0x0DDA8F00  0x00000000 0x64525700  0x2DDA8F00  0
  12 0x642AEA98  0x2DD9F1A0    0xC8550800 0x0DDA9780  0x00000000 0x64525740  0x2DDA9780  0
  13 0x642AEAB8  0x2DD9F1C0    0xC8550800 0x0DDAA000  0x00000000 0x64525780  0x2DDAA000  0
 .
 .
 .
  127 0x642AF8F8  0x2DD9F000    0xC8550800 0x0DDE6900  0x00000000 0x64527400  0x2DDE6900
0
```

Table 1 describes the significant fields shown in the display.

Table 185: show pas y88e8k interface Field Descriptions

Field	Description
ring size	Displays the size of the ring. This is based on the bandwidth of the interface or virtual circuit (VC) and is a power of two.
particle size	Displays the particle size on the receive and transmit paths, in bytes.
ring head	Displays the head of the ring.
tail	Displays the tail of the ring.
rxr	Displays the Rx ring pointer.
next_desc_addr	Displays next Rx buffer descriptor address.
buf_ctrl	Displays the buffer control.
buf_addr_lo	Displays the buffer address.
frame_sw	Displays the Frame status word.
rxr_shadow	Displays the Rx ring shadow.
data_start	Displays the start of data in the particle.
data_bytes	Displays the number of bytes consumed for data storage.

Related Commands

Command	Description
tx-ring-limit	Limits the number of packets that can be used on a transmission ring on the DSL WIC or interface.

show pci aim

To show the IDPROM contents for each compression Advanced Interface Module (AIM) daughter card in the Cisco 2600 router, use the **showpciaim**command in user EXEC or privileged EXEC mode.

show pci aim

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command shows the IDPROM contents for each compression AIM daughtercard present in the system, by AIM slot number (currently 0, since that is the only daughtercard installed for Cisco IOS Release 12.0(1)T). The IDPROM is a small PROM built into the AIM board used to identify it to the system. It is sometimes referred to as an EEPROM because it is implemented using electronically erasable PROM.

Examples

The following example shows the IDPROM output for the installed compression AIM daughter card:

```
Router# show pci aim
AIM Slot 0: ID 0x012D
        Hardware Revision        : 1.0
        EEPROM format version 4
        EEPROM contents (hex):
          0x00: 04 FF 40 01 2D 41 01 00 FF FF FF FF FF FF FF FF
          0x10: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x20: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x30: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x40: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x50: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

Related Commands

Command	Description
clear aim	Clears data compression AIM registers and resets the hardware.
test aim eeprom	Tests the data compression AIM after it is installed in a Cisco 2600 series router.

show platform

To display platform information, use the **show platform** command in privileged EXEC mode.

show platform {**buffers** | **copp rate-limit** {**arp** | **dhcp** | **atm-oam** | **ethernet-oam** | **icmp** | **igmp** | **pppoe-discovery** | **atom ether-vc** | **all**} | **np copp** [*ifnum*] [**detail**] | **dma** | **eeprom** | **fault** | **hardware capacity** | **hardware pfc mode** | **internal-vlan** | **interrupts** | **netint** | **software ipv6-multicast connected** | **stats** | **tech-support** {**ipmulticast** [**vrf** *vrf-name*] *group-ip-addr src-ip-addr* | **unicast** [**vrf** *vrf-name*] *destination-ip-addr destination-mask* [**global**]} | **tlb** | **vfi dot1q-transparency** | **vlans**}

Cisco 4400 Series Integrated Services Routers
show platform

Cisco ASR 1000 Series Aggregation Services Routers
show platform

Syntax Description

buffers	Displays buffer-allocation information.
copp rate-limit	Displays Cisco Control Plane Policing (CoPP) rate-limit information on the Cisco 7600 SIP-400.
arp	Specifies Address Resolution Protocol (ARP) packet traffic.
dhcp	Specifies Dynamic Host Configuration Protocol (DHCP) packet traffic.
atm-oam	Specifies ATM Operation, Administration, and Maintenance (OAM) packet traffic.
ethernet-oam	Specifies Ethernet OAM packet traffic.
icmp	Specifies Internet Connection Management Protoocol Rate limiter.
igmp	Specifies Internet Group Management Potocol Rate limiter.
pppoe-discovery	Specifies Point-to-Point Protocol over Ethernet (PPPoE) discovery packet information.
atom ether-vc	Shows whether IP or routed mode interworking is configured.
all	Displays rate-limit information for all protocols.
np copp	Displays debug information for a given CoPP session ID or for all CoPP sessions.
ifnum	(Optional) A session ID.
detail	(Optional) Shows full rate-limited values.
dma	Displays Direct Memory Access (DMA) channel information.
eeprom	Displays CPU EEPROM information.

fault	Displays the fault date.
hardware capacity	Displays the capacities and utilizations for hardware resources; see the **show platform hardware capacity** command.
hardware pfc mode	Displays the type of installed Policy Feature Card (PFC).
internal-vlan	Displays the internal VLAN.
interrupts	Displays m8500 interrupt counters.
netint	Displays the platform network-interrupt information.
software ipv6-multicast connected	Displays all the IPv6 subnet Access Control List (ACL) entries on the Route Processor (RP); see the show platform software ipv6-multicast command.
stats	Displays Constellation WAN (CWAN) statistics.
tech-support ipmulticast	Displays IP multicast-related information for Technical Assistance Center (TAC).
vrf *vrf-name*	(Optional) Displays the Virtual Private Network (VPN) routing and forwarding (VRF) instance.
group-ip-addr	Group IP address.
src-ip-addr	Source IP address.
unicast	Displays IP unicast-related information for TAC.
destination-ip-addr	Destination IP address.
destination-mask	Destination mask.
global	(Optional) Displays global output.
tlb	Displays information about the translation look-aside buffer (TLB) register.
vfi	Displays CWAN virtual forwarding instance (VFI) commands.
dot1q-transparency	Displays the dot1q transparency setting.
vlans	Displays hidden VLAN-to-WAN interface mapping.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB. This command was changed to include the **hardware pfc mode**keywords.
12.2(18)SXD	This command was modified to include the software ipv6-multicast connectedkeywords.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRC	This command was modified to include additional keywords to support CoPP enhancements on the Cisco 7600 SIP-400 on the Cisco 7600 series router.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRD	This command was modified. The **atom ether-vc** keyword was added.
Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S.
Cisco IOS XE Gibraltar 16.11.1	Output now indicates when a PSU slot is empty. In earlier releases, the state of an empty PSU slot appeared in the command output as "ps, fail". See the examples for differences in indication options for Cisco ASR 1000 Series and ISR 4000 Series routers.

Usage Guidelines

This command is similar to the **show msfc** command.

This command can be used to verify the existence of a second Cisco IOS process on a single Cisco ASR 1000 RP on a Cisco ASR 1002 router or Cisco ASR 1004 router.

When this command is used with the **atom ether-vc** keyword, it is used on the line-card console.

Examples

The following sample output from the **show platform buffers** command displays buffer-allocation information:

```
Router# show platform buffers
Reg. set    Min    Max
  TX               640
 ABQ        640  16384
   0          0     40
   1       6715   8192
   2          0      0
   3          0      0
   4          0      0
   5          0      0
   6          0      0
   7          0      0
Threshold = 8192

Vlan  Sel  Min  Max  Cnt  Rsvd
1019    1 6715 8192    0     0
Router#
```

Cisco ISR 4400 Series Routers

The following example displays online status information for a Cisco ISR 4451-X/K9.

```
Router# show platform
Chassis type: ISR4451-X/K9

Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
0         ISR4451-X/K9        ok                    00:06:51
 0/0      ISR4451-X-4x1GE     ok                    00:05:31
 0/1      NIM-ES2-8-P         ok                    00:05:31
1         ISR4451-X/K9        ok                    00:06:51
 1/0      UCS-EN120S-M2/K9    ok                    00:05:31
2         ISR4451-X/K9        ok                    00:06:51
R0        ISR4451-X/K9        ok, active            00:06:51
F0        ISR4451-X/K9        ok, active            00:06:51
P0        PWR-4450-1000W-AC   ok                    00:06:29
P1        PWR-4450-1000W-AC   ok                    00:06:29
P2        ACS-4450-FANASSY    ok                    00:06:29
POE0      PWR-POE-4450        ok                    00:06:29
GE-POE    PWR-GE-POE-4400     ok                    00:06:29

Slot      CPLD Version        Firmware Version
--------- ------------------- ---------------------------------------
0         15010638            16.7(4r)
1         15010638            16.7(4r)
2         15010638            16.7(4r)
R0        15010638            16.7(4r)
F0        15010638            16.7(4r)
```

The table below describes the fields that appear in the above example

Table 186: show platform Field Descriptions

Field	Description
Slot	Chassis slot number
Type	Type of module
State	Status of the module
Insert time	Period of time ((hh:mm:ss format) since the module has been up and running

Cisco ASR 1000 Series Routers

The following example displays online status information for the shared port adapters (SPAs), Cisco ASR 1000 SPA Interface Processor (SIP), Cisco ASR 1000 Embedded Services Processor (ESP), Cisco ASR 1000 RP, power supplies, and fans. The ESPs are shown as F0 and F1. The RPs are shown as R0 and R1.

The State column should display “ok” for SIPs, SPAs, power supplies, and fans. For RPs and ESPs, the State column should display “ok, active” or “ok, standby.”

```
Router# show platform
```

```
Chassis type: ASR1006
Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
0         ASR1000-SIP10       ok                    18:23:58
 0/0      SPA-5X1GE-V2        ok                    18:22:38
 0/1      SPA-8X1FE-TX-V2     ok                    18:22:33
 0/2      SPA-2XCT3/DS0       ok                    18:22:38
1         ASR1000-SIP10       ok                    18:23:58
 1/0      SPA-2XOC3-POS       ok                    18:22:38
 1/1      SPA-8XCHT1/E1       ok                    18:22:38
 1/2      SPA-2XT3/E3         ok                    18:22:38
R0        ASR1000-RP1         ok, active            18:23:58
R1        ASR1000-RP1         ok, standby           18:23:58
F0        ASR1000-ESP10       ok, active            18:23:58
F1        ASR1000-ESP10       ok, standby           18:23:58
P0        ASR1006-PWR-AC      ok                    18:23:09
P1        ASR1006-FAN         ok                    18:23:09
Slot      CPLD Version        Firmware Version
--------- ------------------- ---------------------------------------
0         06120701            12.2(33r)XN2
1         06120701            12.2(33r)XN2
R0        07082312            12.2(33r)XN2
R1        07082312            12.2(33r)XN2
F0        07051680            12.2(33r)XN2
F1        07051680            12.2(33r)XN2
```

Empty PSU slot

This example shows an "empty" state for slot P1. It applies to Cisco ISR 4000 Series and ASR 1000 Series routers.

```
Device#show platform

Chassis type: ASR1002-X

Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
0         ASR1002-X           ok                    1d18h
 0/0      6XGE-BUILT-IN       ok                    1d18h
 0/1      SPA-8X1GE-V2        ok                    1d18h
R0        ASR1002-X           ok, active            1d18h
F0        ASR1002-X           ok, active            1d18h
P0        ASR1002-PWR-AC      ok                    1d18h
P1        Unknown             empty                 never
```

Cisco ISR 4000 with two PSUs, no power cord attached to P1 or bad input detected

This example shows "fail, badinput" for P1.

On ISR 4000 Series routers, the possible states are:

- "fail, badinput": No power cord attached or bad input detected
- “fail, badoutput”: Bad output detected
- “fail, badcookie”: Failed to read the status of the PSU

```
Device#show platform
```

```
 Chassis type: ISR4431/K9

Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
0         ISR4431/K9          ok                    19:32:35
 0/0      ISR4431-X-4x1GE     ok                    19:30:27
 0/1      NIM-SSD             ok                    19:30:27
R0        ISR4431/K9          ok, active            19:32:35
F0        ISR4431/K9          ok, active            19:32:35
P0        PWR-4430-AC         ok                    19:32:03
P1        Unknown             fail, badinput        19:32:03
P2        ACS-4430-FANASSY    ok                    19:32:03
```

Cisco ASR 1000 with two PSUs, no power cord attached to P1, PSU turned off, or PSU failed

This example shows the "ps, fail" state for slot P1.

```
Device#show platform
Chassis type: ASR1002-X

Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
0         ASR1002-X           ok                    1d18h
 0/0      6XGE-BUILT-IN       ok                    1d18h
 0/1      SPA-8X1GE-V2        ok                    1d18h
R0        ASR1002-X           ok, active            1d18h
F0        ASR1002-X           ok, active            1d18h
P0        ASR1002-PWR-AC      ok                    1d18h
P1        ASR1002-PWR-AC      ps, fail              1d18h
```

Cisco ASR 1000 Series Routers--Verifying Dual Cisco IOS Processes on Single RP

In the following example, a second Cisco IOS process is enabled on a Cisco ASR 1004 router using stateful switchover (SSO). The output of the **show platform** command is provided before and after the SSO configuration to verify that the second Cisco IOS process is enabled and active.

```
Router# show platform
Chassis type: ASR1004
Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
0         ASR1000-SIP10       ok                    00:04:39
 0/0      SPA-5X1GE-V2        ok                    00:03:23
 0/1      SPA-2XT3/E3         ok                    00:03:18
R0        ASR1000-RP1         ok, active            00:04:39
F0        ASR1000-ESP10       ok, active            00:04:39
P0        ASR1004-PWR-AC      ok                    00:03:52
P1        ASR1004-PWR-AC      ok                    00:03:52
Slot      CPLD Version        Firmware Version
--------- ------------------- ---------------------------------------
0         07091401            12.2(33r)XN2
R0        07062111            12.2(33r)XN2
F0        07051680            12.2(33r)XN2
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# redundancy
Router(config-red)# mode sso
*May 27 19:43:43.539: %CMRP-6-DUAL_IOS_REBOOT_REQUIRED: R0/0: cmand:  Configuration must
```

```
be saved and the chassis must be rebooted for IOS redundancy changes to take effect

Router(config-red)# exit
Router(config)# exit
Router#
*May 27 19:44:04.173: %SYS-5-CONFIG_I: Configured from console by user on console

Router# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

Router# reload
Proceed with reload? [confirm]
*May 27 19:45:16.917: %SYS-5-RELOAD: Reload requested by user on console. Reload Reason:
Reload command.
<reload output omitted for brevity>

Router# show platform
Chassis type: ASR1004
Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
0         ASR1000-SIP10       ok                    00:29:34
 0/0      SPA-5X1GE-V2        ok                    00:28:13
 0/1      SPA-2XT3/E3         ok                    00:28:18
R0        ASR1000-RP1         ok                    00:29:34
F0        ASR1000-ESP10       ok, active            00:29:34
P0        ASR1004-PWR-AC      ok                    00:28:47
P1        ASR1004-PWR-AC      ok                    00:28:47
Slot      CPLD Version        Firmware Version
--------- ------------------- ---------------------------------------
0         07091401            12.2(33r)XN2
R0        07062111            12.2(33r)XN2
F0        07051680            12.2(33r)XN2
```

The table below describes the significant fields shown in the display.

Table 187: show platform Field Descriptions

Field	Description
Slot	Chassis slot.
Type	Hardware type.

Field	Description
State	Online state of the hardware. One of the following values: All Hardware • booting--Hardware is initializing and software is booting. • disabled--Hardware is not operational. • init--Hardware or Cisco IOS process is initializing. • ok--Hardware is operational. • shutdown--Hardware was administratively shut down using the no shutdown command. • unknown--Hardware is not operational; state is unknown. RP or ESP • init, standby--Standby RP or ESP is operational but is not yet in a high availability (HA) state. An RP or ESP switchover is not yet possible. • ok, active--Active RP or ESP is operational. • ok, standby--Standby RP or ESP is operational. The standby RP or ESP is ready to become active in the event of a switchover. SPA • admin down--SPA was disabled using the shutdown command. • inserted--SPA is being inserted. • missing--SPA was removed. • out of service--SPA is not operational. • retrieval error--An error occurred while retrieving the SPA state; state is unknown. • stopped--SPA was gracefully deactivated using the hw-module subslot stop command. Fan or Power Supply • fan, fail--Fan is failing. • Empty--Power supply is missing. • ps, fail--Power supply is failing.
Insert time (ago)	Amount of time (hh:mm:ss format) the hardware has been online.
CPLD Version	Complex programmable logic device version number.
Firmware Version	Firmware (ROMmon) version number.

Cisco 7600 Series Routers with Cisco 7600 SIP-400

The following sample output from the **show platform copp rate-limit arp** command displays the list of interfaces on which a rate limiter is active for ARP, along with the count of confirmed and exceeded packets for the rate limiter:

```
Router# show platform copp rate-limit arp
Rate limiter Information for Protocol arp:
  Rate Limiter Status: Enabled
  Rate : 20 pps
  Max Observation Period : 60 seconds
Per Interface Rate Limiter Information
  Interface              Conformed Pkts  Exceeded Pkts  Enabled  Obs Period (Mts)
  GigabitEthernet5/1         0               0            No         -
  GigabitEhternet5/1.1       14              0            No         -
  GigabitEthernet5/1.2       28              2            No         -
  GigabitEthernet5/2         0               0            No         -
  GigabitEthernet5/2.1       180             4            Yes        35
  GigabitEthernet5/2.2       200             16           Yes        Max
```

The table below describes the significant fields shown in the display.

Table 188: show platform copp rate-limit Field Descriptions

Field	Description
Rate Limiter Status	Indicates if a rate limiter has been enabled on the interface.
Rate	Indicates the configured rate in packets per second (pps) or bits per second (bps).
Max Observation Period	Indicates the configured observation period, in seconds, before the per-interface rate limiter is automatically turned off.
Per Interface Rate Limiter Information	Displays the list of interfaces on which the rate limiter is active. In this example: • GigabitEthernet5/1.1 is free from attack. • GigabitEthernet5/2.1 has an exceed count of 4, and has a rate limiter enabled. The observation period is 35 minutes, which indicates that currently the interface is free from attack and is being kept under observation. The interface will remain under observation for an additional 35 minutes. If it remains free from attack after that time, the rate limiter is automatically removed. • GigabitEthernet5/2.2 has an exceed count of 16 and has a rate limiter enabled. The observation period has been designated as Max. This indicates that the interface is still under attack and has not yet entered the observation time window.

The following sample from the **show platform eeprom** command displays CPU EEPROM information:

```
Router# show platform eeprom
MSFC CPU IDPROM:
IDPROM image:
IDPROM image block #0:
  hexadecimal contents of block:
```

```
  00: AB AB 02 9C 13 5B 02 00 00 02 60 03 03 E9 43 69    .....[....`...Ci
  10: 73 63 6F 20 53 79 73 74 65 6D 73 00 00 00 00 00    sco Systems.....
  20: 00 00 57 53 2D 58 36 4B 2D 53 55 50 33 2D 50 46    ..WS-X6K-SUP3-PF
  30: 43 33 00 00 00 00 53 41 44 30 36 34 34 30 31 57    C3....SAD064401W
  40: 4C 00 00 00 00 00 00 00 00 00 37 33 2D 37 34 30    L.........73-740
  50: 34 2D 30 37 00 00 00 00 00 00 30 35 00 00 00 00    4-07......05....
  60: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
  70: 00 00 00 00 02 BD 00 00 00 00 00 09 00 05 00 01    ................
  80: 00 03 00 01 00 01 00 02 03 E9 00 00 00 00 00 00    ................
  90: 00 00 00 00 00 00 00 00 00 00 00 00                ............
  block-signature = 0xABAB, block-version = 2,
  block-length = 156, block-checksum = 4955
  *** common-block ***
  IDPROM capacity (bytes) = 512  IDPROM block-count = 2
  FRU type = (0x6003,1001)
  OEM String = 'Cisco Systems'
  Product Number = 'WS-X6K-SUP3-PFC3'
  Serial Number = 'SAD064401WL'
  Manufacturing Assembly Number = '73-7404-07'
  Manufacturing Assembly Revision = '05'
  Hardware Revision = 0.701
  Manufacturing bits = 0x0  Engineering bits = 0x0
  SNMP OID = 9.5.1.3.1.1.2.1001
  Power Consumption = 0 centiamperes    RMA failure code = 0-0-0-0
  CLEI =
  *** end of common block ***
IDPROM image block #1:
  hexadecimal contents of block:
  00: 60 03 02 67 0C 24 00 00 00 00 00 00 00 00 00 00    `..g.$..........
  10: 00 00 00 00 00 00 00 51 00 05 9A 3A 7E 9C 00 00    .......Q...:~...
  20: 02 02 00 01 00 01 00 00 00 00 00 00 00 00 00 00    ................
  30: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
  40: 14 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
  50: 00 00 81 81 81 81 80 80 80 80 80 80 80 80 80 80    ................
  60: 80 80 06 72 00 46 37                               ...r.F7
  block-signature = 0x6003, block-version = 2,
  block-length = 103, block-checksum = 3108
  *** linecard specific block ***
  feature-bits =   00000000 00000000
  hardware-changes-bits =   00000000 00000000
  card index = 81
  mac base = 0005.9A3A.7E9C
  mac_len = 0
  num_processors = 2
  epld_num = 2
  epld_versions = 0001 0001 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000
  port numbers:
    pair #0: type=14, count=01
    pair #1: type=00, count=00
    pair #2: type=00, count=00
    pair #3: type=00, count=00
    pair #4: type=00, count=00
    pair #5: type=00, count=00
    pair #6: type=00, count=00
    pair #7: type=00, count=00
  sram_size = 0
  sensor_thresholds =
    sensor #0: critical = -127 oC (sensor present but ignored), warning = -127 oC (sensor
present but ignored)
    sensor #1: critical = -127 oC (sensor present but ignored), warning = -127 oC (sensor
present but ignored)
    sensor #2: critical = -128 oC (sensor not present), warning = -128 oC (sensor not
present)
```

```
    sensor #3: critical = -128 oC (sensor not present), warning = -128 oC (sensor not
present)
    sensor #4: critical = -128 oC (sensor not present), warning = -128 oC (sensor not
present)
    sensor #5: critical = -128 oC (sensor not present), warning = -128 oC (sensor not
present)
    sensor #6: critical = -128 oC (sensor not present), warning = -128 oC (sensor not
present)
    sensor #7: critical = -128 oC (sensor not present), warning = -128 oC (sensor not
present)
  max_connector_power = 1650
  cooling_requirement = 70
  ambient_temp = 55
  *** end of linecard specific block ***
```

The following sample output from the **show platform fault** command displays fault-date information:

```
Router# show platform fault
Fault History Buffer:
rsp72043_rp Software (rsp72043_rp-ADVENTERPRISEK9_DBG-M), Version 12.2(32.8.1)RE
C186 ENGINEERING WEEKLY BUILD, synced to V122_32_8_11_SR186
Compiled Wed 08-Apr-09 09:22 by abcd
Uptime 2w3d
Exception Vector: 0x1500 PC 0x0B13DD4C MSR 0x00029200 LR 0x0B13DD10
r0  0x0B13DD10 r1  0x1C58A1C8 r2  0xFFFCFFFC r3  0x189EDEF4
r4  0x00000000 r5  0x00000000 r6  0x1C58A1B0 r7  0x00029200
r8  0x00029200 r9  0x00000000 r10 0x00000001 r11 0x189EDEF0
r12 0x0000001B r13 0x04044000 r14 0x08736008 r15 0x115C0000
r16 0x00000000 r17 0x00000000 r18 0x00000000 r19 0x1B751358
r20 0x00000000 r21 0x00000000 r22 0x00000000 r23 0x00000000
r24 0x00000000 r25 0x00000000 r26 0x00000000 r27 0x00000001
r28 0x13255EC0 r29 0x1C59BD00 r30 0x13255EC0 r31 0x00000000
dec  0x00007333 tbu   0x00004660 tbl   0x594BBFC4 pvr   0x80210020
dear 0x00000000 dbcr0 0x41000000 dbcr1 0x00000000 dbcr2 0x00000000
iac1 0x00000000 iac2  0x00000000 dac1  0x00000000 dac2  0x00000000
```

The following sample output from the **show platform hardware pfc** mode command displays the PFC-operating mode:

```
Router# show platform hardware pfc mode
PFC operating mode : PFC3A
```

This example shows how to display platform network-interrupt information:

```
Router# show platform netint
Network IO Interrupt Throttling:
 throttle count=0, timer count=0
 active=0, configured=1
 netint usec=3999, netint mask usec=800
inband_throttle_mask_hi = 0x0
inband_throttle_mask_lo = 0x800000
```

This following sample output from the **show platform tlb** command displays the TLB-register information:

```
Router# show platform tlb
Mistral revision 5
TLB entries : 42
Virt Address range      Phy Address range      Attributes
0x10000000:0x1001FFFF   0x010000000:0x01001FFFF   CacheMode=2, RW, Valid
0x10020000:0x1003FFFF   0x010020000:0x01003FFFF   CacheMode=2, RW, Valid
0x10040000:0x1005FFFF   0x010040000:0x01005FFFF   CacheMode=2, RW, Valid
```

```
0x10060000:0x1007FFFF   0x010060000:0x01007FFFF   CacheMode=2, RW, Valid
0x10080000:0x10087FFF   0x010080000:0x010087FFF   CacheMode=2, RW, Valid
0x10088000:0x1008FFFF   0x010088000:0x01008FFFF   CacheMode=2, RW, Valid
0x18000000:0x1801FFFF   0x010000000:0x01001FFFF   CacheMode=0, RW, Valid
0x19000000:0x1901FFFF   0x010000000:0x01001FFFF   CacheMode=7, RW, Valid
0x1E000000:0x1E1FFFFF   0x01E000000:0x01E1FFFFF   CacheMode=2, RW, Valid
0x1E880000:0x1E899FFF   0x01E880000:0x01E899FFF   CacheMode=2, RW, Valid
0x1FC00000:0x1FC7FFFF   0x01FC00000:0x01FC7FFFF   CacheMode=2, RO, Valid
0x30000000:0x3001FFFF   0x070000000:0x07001FFFF   CacheMode=2, RW, Valid
0x40000000:0x407FFFFF   0x000000000:0x0007FFFFF   CacheMode=3, RO, Valid
.
.
.
0x58000000:0x59FFFFFF   0x088000000:0x089FFFFFF   CacheMode=3, RW, Valid
0x5A000000:0x5BFFFFFF   0x08A000000:0x08BFFFFFF   CacheMode=3, RW, Valid
0x5C000000:0x5DFFFFFF   0x08C000000:0x08DFFFFFF   CacheMode=3, RW, Valid
0x5E000000:0x5FFFFFFF   0x08E000000:0x08FFFFFFF   CacheMode=3, RW, Valid
```

This example shows how use the **atom ether-vc** keyword to display line-card information for an ES20 line card in slot 3.

```
Router# show platform copp rate-limit atom ether-vc
 AToM Ether VC Index(12902): segtype(3) seghandle(0x5ECF7F34)
  Disposition : flags(97) vlanid(502) local_vc_label(22691)
   ForwardingTable: oper(12) flags(0x2100) vlan(502) dest_index(0x9ED)
  Imposition: flags(0x21) egress_idx(0x0) ifnum(28)
   tx_tvc(0x7D83) rvclbl[0](3356) rigplbl[1](1011) label[2](0)
   label[3](0) ltl(0x9ED) mac(0014.1c80.f600) qos_info(0x0)
  Platform Data:
   loc_lbl acif_num fw_idx cword    eg_ifnum ckt_idx  vlan ac_hdl     vc_hash
   22691   615      0x0    0x3      28       0x8003   502  0x5ECF7F34 0x3266
  Platform Index(0x81F68003) is_sw(1) is_vfi(0) vlan(502) pseudo_port_offset(3) tx_tvc(0x7D83)

  Statistics :  Packets    Bytes      Drop Pkts  Drop Bytes ID
   Disposition: 0          0          0          0          0
   Imposition : 0          0          0          0          0
     Vlan func[1]: 502 (0x1F6) func(0:invalid) feat  (0x0 )
    Tx TVC Table
            idx   ltl h pt cw vt efp  adj  v imp
            x---- x-- d d- d- d- x--- x--- d x---
  SIP10G EoMPLS disp detailed info:
    t vclbl    VLAN       Type    disp-idx
    - d------- x---(d---) ------- x-------
    0 00022691 01F6(0502) ether   00001692
  SIP10G EoMPLS ipiw disp detailed info:
    ipiw mac valid CE-MAC Address
    b--- b-------- --------------
    0001 000000001 0016.9c6e.7480
  VC Summary: vlan(502) VC count(1)
```

Related Commands

Command	Description
platform copp	Turns on or off rate-limiting for an interface on the Cisco 7600 SIP-400.
platform copp observation period	Sets the observation period before automatically turning off the per-interface rate limiter on the Cisco 7600 SIP-400.
pseudowire class	Specifies the name of a Layer 2 pseudowire class.

Command	Description
show msfc	Displays MSFC information.

show platform acl software-switched

To display whether ACLs are enabled for software-switched WAN packets, use the **showplatformaclsoftware-switched**command in privileged EXEC mode.

show platform acl software-switched

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
12.2(33)SXI2	This command was integrated into Cisco IOS Release 12.2(33)SXI2.

Usage Guidelines

By default, ACLs are not applied to packets that are software-switched between WAN cards and the route processor. To determine whether ACLs are enabled for software-switched ingress or egress WAN packets, use the **showplatformaclsoftware-switched**command.

Examples

This example shows how to display whether ACLs are enabled for software-switched WAN packets:

```
Router# show platform acl software-switched
 CWAN: ACL treatment for software switched in INGRESS is enabled
 CWAN: ACL treatment for software switched in EGRESS is disabled
```

Related Commands

Command	Description
platform cwan acl software-switched	Allows ACLs to be applied to WAN packets that are software-switched.

show platform atom disp-tbl backup

To display the disposition table on the line card for backup VCs, use the **showplatformatomdisp-tblbackup** command in privileged EXEC mode .

show platform atom disp-tbl backup *pseudo-ckt-index*

Syntax Description

pseudo-ckt-index	Defines the *pseudo-circuit-index*. The acceptable range is between 1 and 65537.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)S	This command was introduced.

Usage Guidelines

The show platform atom disp-tbl backup command should be used while using the Hot-Standby Psuedo Wire (HSPW) feature.

Examples

The following example displays the disposition table on the Line Card for backup VCs.

```
Router# show platform atom disp-tbl backup

Pseudo   Dlci or   Local         Outgoing          IW   Backup
Ckt Idx    Vcd     Label         Interface        Type   VC
-------  -------  -------  ---------------------  ----  ------
  32786       2       24                    AC0   L2L    Yes
```

Related Commands

Command	Description
show platform atom disp-tbl local-vc-label	Displays the disposition table on the line card for a VC based on the local label.
show platform atom tbl-summary	Displays the total number of PWs programmed on the Line Card.
show platform atom imp-tbl backup	Displays the imposition table on the line card for backup VCs.
show platform atom imp-tbl remote-vc-label	Displays the imposition table on the line card for a VC based on the remote label.

show platform atom disp-tbl local-vc-label

To display the disposition table on the line card for a VC based local label, use the **showplatformatomdisp-tbllocal-vc-label** command in privileged EXEC mode .

show platform atom disp-tbl local-vc-label *local-vc-label*

Syntax Description

local-vc-label	Defines the VC based local label. The acceptable range is between 15 and 1048575.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)S	This command was introduced.

Usage Guidelines

The show platform atom disp-tbl local-vc-label command should be used only if you know the Local VC Label for a VC.

Examples

The following example displays the disposition table on the Line Card for a VC based on the local label.

```
Router# show platform atom imp-tbl remote-vc-label 97
Pseudo Ckt Idx    Dlci or Vcd   Dest Vlanid   LTL Index   # Lbls Imposed   Remote Label
--------------   -------------  ------------  ----------  ---------------  --------------
 49170               2           1028          0xFF             2              97
Local Label  Outgoing Interface   IW Type  Backup VC    AC segment ssm id   Segment Status
----------- --------------------  -------  ---------   -------------------  --------------

   57             Gi4/3/3          L2L       No           20561                 UP
```

Related Commands

Command	Description
show platform atom imp-tbl remote-vc-label	Displays the imposition table on the line card for a VC based on the remote label.
show platform atom tbl-summary	Displays the total number of PWs programmed on the line card.
show platform atom imp-tbl backup	Displays the imposition table on the line card for backup VCs.
show platform atom disp-tbl backup	Displays the disposition table on the line card for backup VCs.

show platform atom imp-tbl backup

To display the imposition table on the line card for backup VCs, use the **showplatformatomimp-tblbackup** command in privileged EXEC mode .

show platform atom imp-tbl backup *pseudo-ckt-index*

Syntax Description

pseudo-ckt-index	Defines the *pseudocircuitindex*. The acceptable range is between 1 and 65537.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)S	This command was introduced.

Usage Guidelines

The show platform atom imp-tbl backup command should be used while using the Hot-Standby Psuedo Wire (HSPW) feature.

Examples

The following example displays the imposition table on the Line Card for backup VCs.

```
Router# show platform atom imp-tbl backup

Pseudo Ckt Idx    Dlci or Vcd   Dest Vlanid   LTL Index   # Lbls Imposed   Remote Label
--------------   -------------  ------------  ----------  ---------------  --------------
 432786      2            1029        0xFF            1        25
Local Label  Outgoing Interface   IW Type  Backup VC    AC segment ssm id   Segment Status
----------- --------------------  -------  ---------   -------------------  --------------

61      Gi4/0/1    L2L       Yes      16464      STANDBY
```

Related Commands

Command	Description
show platform atom disp-tbl local-vc-label	Displays the disposition table on the line card for a VC based on the local label.
show platform atom tbl-summary	Displays the total number of PWs programmed on the Line Card.
show platform atom disp-tbl backup	Displays the disposition table on the line card for backup VCs.
show platform atom imp-tbl remote-vc-label	Displays the imposition table on the line card for a VC based on the remote label.

show platform atom imp-tbl remote-vc-label

To display the imposition table on the line card for a VC based remote label, use the **showplatformatomimp-tblremote-vc-label** command in privileged EXEC mode .

show platform atom imp-tbl *remote-vc-label remote-vc-label*

Syntax Description

remote-vc-label	Defines the remote VC based label. The acceptable range is between 15 and 1048575.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)S	This command was introduced.

Usage Guidelines

The **showplatformatomimp-tblremote-vc-label** command should be used only if the Remote VC Label for a VC is known.

Examples

The following example displays the imposition table on the Line Card for a VC based on the remote label.

```
Router# show platform atom imp-tbl remote-vc-label 97
Pseudo Ckt Idx    Dlci or Vcd   Dest Vlanid   LTL Index   # Lbls Imposed   Remote Label
--------------   -------------  ------------  ----------  ---------------  --------------
 49170                2           1028          0xFF            2               97
Local Label  Outgoing Interface   IW Type  Backup VC    AC segment ssm id   Segment Status
----------- --------------------  -------  ---------   -------------------  --------------

   57            Gi4/3/3         L2L      No           20561                UP
```

Related Commands

Command	Description
show platform atom disp-tbl local-vc-label	Displays the disposition table on the line card for a VC based on the local label.
show platform atom tbl-summary	Displays the total number of PWs programmed on the Line Card.
show platform atom imp-tbl backup	Displays the imposition table on the line card for backup VCs.
show platform atom disp-tbl backup	Displays the disposition table on the line card for backup VCs.

show platform atom tbl-summary

To display the total number of pseudowires (PWs) programmed on the line card., use the**showplatformatomtbl-summary** command in privileged EXEC mode .

show platform atom tbl-summary

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)S	This command was introduced.

Usage Guidelines

The **showplatformatomtbl-summary** command is used to determine the primaryPWs and backup PWs that are programmed.

Examples

This example displays the total number of PWs programmed on the Line Card.

```
Router# show platform atom tbl-summary

 Total Number of entries(CWAN): 2, AToM Entries(LC): 2 Local Switching Entries(LC): 0
 AToM Entries Primary: 1, Backup: 1
```

Related Commands

Command	Description
show platform atom imp-tbl local-vc-label	Displays the imposition table on the line card for a VC based on the remote label.
show platform atom disp-tbl local-vc-label	Displays the disposition table on the line card for a VC based on the local label.
show platform atom imp-tbl backup	Displays the imposition table on the line card for backup VCs.
show platform atom disp-tbl backup	Displays the disposition table on the line card for backup VCs.

show platform condition

To display the currently active debug configuration, use the **show platform condition** command in privileged EXEC mode.

show platform condition

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 3.10.0S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Example

The following is sample output of the **show platform condition** command:

```
Router# show platform condition

Conditional Debug Global State: Start

Conditions                                                            Direction
----------------------------------------------------------------------|---------
VoIP-Null0                                & IPV4 [2.2.2.2/24]         both
LI-Null0                                  & IPV4 [2.2.2.2/24]         both
GigabitEthernet0                          & IPV4 [2.2.2.2/24]         both
LIIN0                                     & IPV4 [2.2.2.2/24]         both
GigabitEthernet0/0/0                      & IPV4 [2.2.2.2/24]         both
GigabitEthernet0/0/1                      & IPV4 [2.2.2.2/24]         both
GigabitEthernet0/1/0                      & IPV4 [2.2.2.2/24]         both
GigabitEthernet0/1/1                      & IPV4 [2.2.2.2/24]         both
GigabitEthernet0/3/0                      & IPV4 [2.2.2.2/24]         both
GigabitEthernet0/3/1                      & IPV4 [2.2.2.2/24]         both
GigabitEthernet0/3/6                      & IPV4 [2.2.2.2/24]         both
GigabitEthernet0/3/7                      & IPV4 [2.2.2.2/24]         both
Loopback1                                 & IPV4 [2.2.2.2/24]         both
Overlay10                                 & IPV4 [2.2.2.2/24]         both
Overlay30                                 & IPV4 [2.2.2.2/24]         both
GigabitEthernet0/0/4.20                   & IPV4 [2.2.2.2/24]         both
Internal-RP                               & IPV4 [2.2.2.2/24]         both
Internal-Recycle                          & IPV4 [2.2.2.2/24]         both
GigabitEthernet0/0/2.EFP100               & IPV4 [2.2.2.2/24]         both
```

The following table describes the significant fields shown in the display.

Table 189: show platform condition Field Descriptions

Field	Description
Conditions	Condition of platform debug.
Direction	Direction of platform debug.

show platform diag

To display diagnostic and debug information about individual platform components, use the **show platform diag** command in privileged EXEC mode.

show platform diag

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.2	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S.

Usage Guidelines

This command can be used to display the debug and diagnostic information about the Cisco ASR 1000 shared port adapter (SPA) Interface Processor (SIP), SPA, Cisco ASR 1000 Embedded Services Processor (ESP), Cisco ASR 1000 Route Processor (RP), and power supplies. This command also indicates the status of the field replaceable unit (FRU) components in any Cisco ASR 1000 Series Router.

Use the **show platform diag** command to display the debug and diagnostic information related to your Cisco 4400 Series Integrated Services Router (ISR), any connected Service Modules (SM-X) or Network Interface Modules (NIMs), power supply for front panel Gigabit Ethernet (FPGE) ports, Fan Trays and other components of your router.

Examples

The following is sample output from the **show platform diag** command. The Embedded Services Processor (ESP) is shown as F0 or F1. The RPs are shown as R0 or R1. The power supplies are shown as P0 and P1.

```
Device# show platform diag

Chassis type: ASR1004
Slot: 0, ASR1000-SIP10
Running state               : ok
Internal state              : online
Internal operational state  : ok
Physical insert detect time : 00:00:48 (4d22h ago)
Software declared up time   : 00:01:40 (4d22h ago)
CPLD version                : 07091401
Firmware version            : 12.2(33r)XNB
Sub-slot: 0/0, SPA-5X1GE-V2
Operational status          : ok
Internal state              : inserted
Physical insert detect time : 00:00:36 (4d22h ago)
Logical insert detect time  : 00:02:23 (4d22h ago)
Sub-slot: 0/1, SPA-2XT3/E3
Operational status          : ok
Internal state              : inserted
  Physical insert detect time : 00:00:36 (4d22h ago)
  Logical insert detect time  : 00:02:23 (4d22h ago)
```

```
Slot: R0, ASR1000-RP1
  Running state               : ok
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:00:48 (4d22h ago)
  Software declared up time   : 00:00:48 (4d22h ago)
  CPLD version                : 07062111
  Firmware version            : 12.2(33r)XNB
Sub-slot: R0/0,
  Running state               : ok, active
  Logical insert detect time  : 00:00:48 (4d22h ago)
  Became HA Active time       : 00:04:56 (4d22h ago)
Sub-slot: R0/1,
  Running state               : ok, standby
  Logical insert detect time  : 00:02:50 (4d22h ago)
Slot: F0, ASR1000-ESP10
  Running state               : ok, active
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:00:48 (4d22h ago)
  Software declared up time   : 00:01:40 (4d22h ago)
  Hardware ready signal time  : 00:00:49 (4d22h ago)
  Packet ready signal time    : 00:01:49 (4d22h ago)
  CPLD version                : 07051680
  Firmware version            : 12.2(33r)XNB
Slot: P0, ASR1004-PWR-AC
  State                       : ok
  Physical insert detect time : 00:01:40 (4d22h ago)
Slot: P1, ASR1004-PWR-AC
  State                       : ok
  Physical insert detect time : 00:01:40 (4d22h ago)
```

```
Device# show platform diag

Chassis type: CSR1000V

Slot: R0, CSR1000V
  Running state               : ok, active
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:00:37 (00:02:26 ago)
  Software declared up time   : 00:00:37 (00:02:26 ago)

Slot: F0, CSR1000V
  Running state               : ok, active
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:00:37 (00:02:26 ago)
  Software declared up time   : 00:00:57 (00:02:06 ago)
  Hardware ready signal time  : 00:00:56 (00:02:06 ago)
  Packet ready signal time    : 00:01:01 (00:02:02 ago)
```

Cisco 4400 Series Integrated Services Router: Example

The following is a sample output from the **show platform diag** command.

```
Router# show platform diag

Chassis type: ISR4451/K9

Slot: 0, ISR4451/K9
```

```
  Running state               : ok
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:01:05 (6d23h ago)
  Software declared up time   : 00:01:46 (6d23h ago)
  CPLD version                : 12090323
  Firmware version           : 12.2(20120829:165313) [ciscouser-ESGROM_20120829_DELTA 101]


Sub-slot: 0/0, ISR4451-X-4x1GE
  Operational status          : ok
  Internal state              : inserted
  Physical insert detect time : 00:02:57 (6d23h ago)
  Logical insert detect time  : 00:02:57 (6d23h ago)

Slot: 1, ISR4451/K9
  Running state               : ok
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:01:05 (6d23h ago)
  Software declared up time   : 00:01:47 (6d23h ago)
  CPLD version                : 12090323
  Firmware version           : 12.2(20120829:165313) [ciscouser-ESGROM_20120829_DELTA 101]


Sub-slot: 1/0, SM-X-1T3/E3
  Operational status          : ok
  Internal state              : inserted
  Physical insert detect time : 00:02:57 (6d23h ago)
  Logical insert detect time  : 00:02:57 (6d23h ago)

Slot: 2, ISR4451/K9
  Running state               : ok
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:01:05 (6d23h ago)
  Software declared up time   : 00:01:48 (6d23h ago)
  CPLD version                : 12090323
  Firmware version           : 12.2(20120829:165313) [ciscouser-ESGROM_20120829_DELTA 101]


Slot: R0, ISR4451/K9
  Running state               : ok, active
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:01:05 (6d23h ago)
  Software declared up time   : 00:01:05 (6d23h ago)
  CPLD version                : 12090323
  Firmware version           : 12.2(20120829:165313) [ciscouser-ESGROM_20120829_DELTA 101]


Slot: F0, ISR4451/K9
  Running state               : ok, active
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:01:05 (6d23h ago)
  Software declared up time   : 00:02:20 (6d23h ago)
  Hardware ready signal time  : 00:00:00 (never ago)
  Packet ready signal time    : 00:02:29 (6d23h ago)
  CPLD version                : 12090323
  Firmware version           : 12.2(20120829:165313) [ciscouser-ESGROM_20120829_DELTA 101]


Slot: P0, Unknown
```

```
  State                        : ps, fail
  Physical insert detect time : 00:00:00 (never ago)

Slot: P1, XXX-XXXX-XX
  State                        : ok
  Physical insert detect time : 00:01:30 (6d23h ago)

Slot: P2, ACS-4450-FANASSY
  State                        : ok
  Physical insert detect time : 00:01:30 (6d23h ago)

Slot: GE-POE, Unknown
  State                        : NA
  Physical insert detect time : 00:00:00 (never ago)
```

The table below describes the significant fields shown in the display.

Table 190: show platform diag Field Descriptions

Field	Description
Running state	The current online running state of the FRU component.
Internal state	The internal debug state of the FRU component for diagnostic purposes.
Internal operational state	The internal operational state of the FRU component for diagnostic purposes.
Physical insert detect time	The time of the most recent physical insertion of the FRU component detected by the platform code.
Software declared up time	The time that the software on the FRU component was declared running by the platform code.
Hardware ready signal time	The time that the hardware ready signal was detected by the platform code.
Packet ready signal time	The time that the ESP packet ready signal was detected by the platform code.
CPLD version	The Complex Programmable Logic Device (CPLD) version number.
Firmware version	The firmware ROM monitor (ROMMON) version number.
Logical insert detect time	The time that the SPA was logically detected by the platform code.
Became HA Active time	The time that this FRU became High Availability (HA) active.

Related Commands

Command	Description
show platform	Displays platform information.
show platform hardware	Displays platform hardware information.
show platform software	Displays platform software information.

show platform discover-devices

To display PCI device information, use the **showplatformdiscover-devices**command in privileged EXEC mode.

show platform discover-devices

Syntax Description

show platform discover-devices	Displays PCI device information.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
15.1(1)T	This command was introduced for Cisco 3925E and Cisco 3945E Integrated Services Routers.

Usage Guidelines

Use the **showplatformdiscover-devices** command to display information about PCI devices on the router. The output shows the device name, interface slot and port, and detailed hardware information.

Examples

The following sample output shows PCI device information for Cisco 3925E ISR.

```
Router#show platform discover-devices
Discovered PCI device GE 0/0, GE 0/1
  root_port=2, bus_no=1, device_no=0, func_no=0, root_device_id=2
  DeviceID=0x10C9, VendorID=0x8086, Command=0x0146, Status=0x0010
  Class=0x02/0x00/0x00, Revision=0x01, LatencyTimer=0x00, CacheLineSize=0x10
  BaseAddr0=0xFD220000, BaseAddr1=0x00000000
Discovered PCI device GE 0/2, GE 0/3
  root_port=3, bus_no=2, device_no=0, func_no=0, root_device_id=3
  DeviceID=0x10C9, VendorID=0x8086, Command=0x0146, Status=0x0010
  Class=0x02/0x00/0x00, Revision=0x01, LatencyTimer=0x00, CacheLineSize=0x10
  BaseAddr0=0xFD120000, BaseAddr1=0x00000000
Discovered PCI device PLX:
  root_port=6, bus_no=37, device_no=0, func_no=0, root_device_id=6
  DeviceID=0x8509, VendorID=0x10B5, Command=0x0007, Status=0x0010
  Class=0x06/0x04/0x00, Revision=0xAA, LatencyTimer=0x00, CacheLineSize=0x10
  BaseAddr0=0xF8F00000, BaseAddr1=0x00000000
  SecLat=0x00, SubBus=53, SecBus=38, PrimBus=37
  MemLimit=0xF8F0, MemBase=0xF100, PrefMemLimit=0x0001, PrefMemBase=0xFFF1
Discovered PCI device PLX:
  root_port=6, bus_no=38, device_no=1, func_no=0, root_device_id=6
  DeviceID=0x8509, VendorID=0x10B5, Command=0x0007, Status=0x0010
  Class=0x06/0x04/0x00, Revision=0xAA, LatencyTimer=0x00, CacheLineSize=0x10
  BaseAddr0=0x00000000, BaseAddr1=0x00000000
  SecLat=0x00, SubBus=40, SecBus=39, PrimBus=38
  MemLimit=0xF2F0, MemBase=0xF100, PrefMemLimit=0x0001, PrefMemBase=0xFFF1
```

Table 191: Show Platform Discover-Devices Field Description

Field	Description
PCI Device	Identifies the PCI device on the router.
Root_port	Defines the root port address on the device.

Field	Description
Bus_no	Defines the bus number on the device.
Device_no	Defines the device number.
Func_no	Defines the function number.
Root_device_id	Defines the root device number.
DeviceID	Defines the device identifcation number.
VendorID	Defines the vendor identifcation number.
Operation Command	Defines the operation command.
Status of Device	Defines the status of device.
Class	Defines the class address.
Revision (type of device)	Defines type of device.
LatencyTimer	Defines the latency timer.
CacheLineSize	Defines cache line size.
Base Address	Address of Base.
Base Address 1	Address of Base 1.
Secondary Latency Timer	Defines secondary latency timer.
SubBus	Defines subordinate Bus number.
SecBus	Defines secondary Bus number.
PrimBus	Defines primary Bus number.
DeviceID	Defines the device identifcation number.
MemLimit	Defines the memory limit.
MemBase	Defines the memory base.
PrefMemLimit	Defines the pre-fetchable memory limit.
PrefMemBase	Defines the pre-fetchable memory base.

Related Commands

Command	Description
show platform cf	Shows CF support-related information.
show platform dma	Show DMA-related information.
show platform hw-module-power	Displays power settings of service modules.

Command	Description
show platform interrupt	Shows Interrupt-related information.
show platform io-controller	Displays IO-controller information.
show platform led	Shows LED-related information.
show platform nvram	Displays NVRAM-related information.
show platform versions	Displays versions/revisions of various modules.
show platform smbdev	Shows smbus slave devices.
show platform mgf	Shows multi-gigabit fabric information.

show platform dwdm alarm history

To display platform DWDM alarm history, use the **showplatformdwdmalarmhistory**command in privileged EXEC mode.

show platform dwdm alarm history [**port index**]

Syntax Description

port index	Specifies the port index. • For a 7600-ES+ITU-2TG, the valid values for the port index are 1, 2. • For a 7600-ES+ITU-4TG, the valid values for the port index are 1, 2, 3, 4.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRD1	This command was introduced on the Cisco 7600 series routers for the 7600-ES+ITU-2TG and the 7600-ES+ITU-4TG line cards only.

Usage Guidelines

If the port index is not specified, the alarm history (last 32 alarms) for all ports on that line card whose interface transport mode is Optical Transport Network (OTN) is displayed. If a port index is specified, the alarm history (last 32 alarms) for that particular port is displayed, if the interface transport mode of that port is OTN. An alarm is logged in the alarm history only if the reporting for that alarm is enabled. If reporting for an alarm is disabled with the no g709 otu report command or the no g709 odu report command, then neither the alarm declaration nor clearing will be logged in the alarm history.

Examples

The following examples illustrate the command when interface TenGigabitEthernet 2/1 and interface TenGigabitEthernet 2/3 are configured with a transport-mode of OTN. Because the transport modes of interface TenGigabitEthernet 2/2 and interface TenGigabitEthernet 2/4 are not OTN, nothing is displayed for dwdm 2/2 and dwdm 2/4.

```
Router# show platform dwdm alarm history
dwdm 2/1 :
Current alarms in HW are
 LOS
 ---- LAST 32 ALARMS ----------
00. LOS declared                    , *Jan  7 2009 21:16:40.165 UTC
dwdm 2/3 :
Current alarms in HW are

 ---- LAST 32 ALARMS ----------
00. LOS cleared                     , *Jan  7 2009 21:14:32.709 UTC
01. LOS declared                    , *Jan  7 2009 21:14:02.625 UTC
Router# show platform dwdm alarm history 1
dwdm 2/1 :
Current alarms in HW are
 LOS
 ---- LAST 32 ALARMS ----------
00. LOS declared                    , *Jan  7 2009 21:16:40.165 UTC
Router# how platform dwdm alarm history 2
```

```
Router# show platform dwdm alarm history 3
dwdm 2/3 :
Current alarms in HW are

 ---- LAST 32 ALARMS ----------
00. LOS cleared                     , *Jan  7 2009 21:14:32.709 UTC
01. LOS declared                    , *Jan  7 2009 21:14:02.625 UTC
```

Related Commands

Command	Description
show controllers dwdm	Displays ITU-T G.709 alarms, alerts, and counters for a DWDM controller.

show platform hardware capacity

To display the capacities and utilizations for the hardware resources, use the **show platform hardware capacity** command in privileged EXEC mode.

show platform hardware capacity [*resource-type*]

Syntax Description

resource-type	(Optional) Hardware resource type; see the "Usage Guidelines" section for the valid values.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)SXF	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. Support was added for the **ibc** and **rewrite-engine** keywords.

Usage Guidelines

The valid values for *resource-type* are as follows:

- **acl** --Displays the capacities and utilizations for ACL/QoS TCAM resources.
- **cpu** --Displays the capacities and utilizations for CPU resources.
- **eobc** --Displays the capacities and utilizations for Ethernet out-of-band channel resources.
- **fabric** --Displays the capacities and utilizations for Switch Fabric resources.
- **flash** --Displays the capacities and utilizations for Flash/NVRAM resources.
- **forwarding** --Displays the capacities and utilizations for Layer 2 and Layer 3 forwarding resources.
- **ibc** --Displays the capacities and utilizations for interboard communication resources.
- **interface** --Displays the capacities and utilizations for interface resources.
- **monitor** --Displays the capacities and utilizations for SPAN resources.
- **multicast** --Displays the capacities and utilizations for Layer 3 multicast resources.
- **netflow** --Displays the capacities and utilizations for NetFlow resources.
- **pfc** --Displays the capacities and utilizations for all the PFC resources including Layer 2 and Layer 3 forwarding, NetFlow, CPU rate limiters, and ACL/QoS TCAM resources.
- **power** --Displays the capacities and utilizations for power resources.
- **qos** --Displays the capacities and utilizations for QoS policer resources.
- **rate-limit** --Displays the capacities and utilizations for CPU rate limiter resources.

- **rewrite-engine** --Displays the packet drop and performance counters of the central rewrite engine on supervisors and line cards. For detailed information, see the **show platform hardware capacity rewrite-engine** command documentation.
- **system** --Displays the capacities and utilizations for system resources.
- **vlan** --Displays the capacities and utilizations for VLAN resources.

The **show platform hardware capacity cpu**command displays the following information:

- CPU utilization for the last 5 seconds (busy time and interrupt time), the percentage of the last 1-minute average busy time, and the percentage of the last 5-minute average busy time.
- Processor memory total available bytes, used bytes, and percentage used.
- I/O memory total available bytes, used bytes, and percentage used.

The **show platform hardware capacity eobc**command displays the following information:

- Transmit and receive rate
- Packets received and packets sent
- Dropped received packets and dropped transmitted packets

The **show platform hardware capacity forwarding** command displays the following information:

- The total available entries, used entries, and used percentage for the MAC tables.
- The total available entries, used entries, and used percentage for the FIB TCAM tables. The display is done per protocol base.
- The total available entries, used entries, and used percentage for the adjacency tables. The display is done for each region in which the adjacency table is divided.
- The created entries, failures, and resource usage percentage for the NetFlow TCAM and ICAM tables.
- The total available entries and mask, used entries and mask, reserved entries and mask, and entries and mask used percentage for the ACL/QoS TCAM tables. The output displays the available, used, reserved, and used percentage of the labels. The output displays the resource of other hardware resources that are related to the ACL/QoS TCAMs (such as available, used, reserved, and used percentage of the LOU, ANDOR, and ORAND).
- The available, used, reserved, and used percentage for the CPU rate limiters.

The **show platform hardware capacity interface** command displays the following information:

- Tx/Rx drops--Displays the sum of transmit and receive drop counters on each online module (aggregate for all ports) and provides the port number that has the highest drop count on the module.
- Tx/Rx per port buffer size--Summarizes the port-buffer size on a per-module basis for modules where there is a consistent buffer size across the module.

The **show platform hardware capacity monitor** command displays the following SPAN information:

- The maximum local SPAN sessions, maximum RSPAN sessions, maximum ERSPAN sessions, and maximum service module sessions.

- The local SPAN sessions used/available, RSPAN sessions used/available, ERSPAN sessions used/available, and service module sessions used/available.

The **show platform hardware capacity multicast** command displays the following information:

- Multicast Replication Mode: ingress and egress IPv4 and IPv6 modes.
- The MET table usage that indicates the total used and the percentage used for each module in the system.
- The bidirectional PIM DF table usage that indicates the total used and the percentage used.

The **show platform hardware capacity system**command displays the following information:

- PFC operating mode (PFC Version: PFC3A, PFC3B, unknown, and so forth)
- Supervisor redundancy mode (RPR, RPR+, SSO, none, and so forth)
- Module-specific switching information, including the following information:
    - Part number (WS-SUP720-BASE, WS-X6548-RJ-45, and so forth)
    - Series (supervisor engine, fabric, CEF720, CEF256, dCEF256, or classic)
    - CEF Mode (central CEF, dCEF)

The **show platform hardware capacity vlan** command displays the following VLAN information:

- Total VLANs
- VTP VLANs that are used
- External VLANs that are used
- Internal VLANs that are used
- Free VLANs

Examples

This example shows how to display CPU capacity and utilization information for the route processor, the switch processor, and the LAN module in the Cisco 7600 series router:

```
Router# show platform hardware capacity cpu
CPU Resources
  CPU utilization: Module             5 seconds       1 minute       5 minutes
                   1  RP               0% /  0%             1%              1%
                   1  SP               5% /  0%             5%              4%
                   7                  69% /  0%            69%             69%
                   8                  78% /  0%            74%             74%
  Processor memory: Module   Bytes:       Total           Used           %Used
                    1  RP             176730048       51774704             29%
                    1  SP             192825092       51978936             27%
                    7                 195111584       35769704             18%
                    8                 195111584       35798632             18%
  I/O memory: Module         Bytes:       Total           Used           %Used
              1  RP                    35651584       12226672             34%
              1  SP                    35651584        9747952             27%
              7                        35651584        9616816             27%
              8                        35651584        9616816             27%
Router#
```

This example shows how to display EOBC-related statistics for the route processor, the switch processor, and the DFCs in the Cisco 7600 series router:

```
Router# show platform hardware capacity eobc
EOBC Resources
  Module                     Packets/sec     Total packets     Dropped packets
  1  RP      Rx:                      61            108982                   0
             Tx:                      37             77298                   0
  1  SP      Rx:                      34            101627                   0
             Tx:                      39            115417                   0
  7          Rx:                       5             10358                   0
             Tx:                       8             18543                   0
  8          Rx:                       5             12130                   0
             Tx:                      10             20317                   0
Router#
```

This example shows how to display the current and peak switching utilization:

```
Router# show platform hardware capacity fabric
Switch Fabric Resources
  Bus utilization: current is 100%, peak was 100% at 12:34 12mar45
  Fabric utilization:      ingress                     egress
      Module channel speed current peak                current peak
       1      0        20G   100%  100% 12:34 12mar45  100%    100% 12:34 12mar45
       1      1        20G   12%    80% 12:34 12mar45   12%     80% 12:34 12mar45
       4      0        20G   12%    80% 12:34 12mar45   12%     80% 12:34 12mar45
      13      0         8G   12%    80% 12:34 12mar45   12%     80% 12:34 12mar45
Router#
```

This example shows how to display information about the total capacity, the bytes used, and the percentage that is used for the Flash/NVRAM resources present in the system:

```
Router# show platform hardware capacity flash
Flash/NVRAM Resources
  Usage: Module Device               Bytes:      Total          Used     %Used
         1  RP  bootflash:                    31981568      15688048       49%
         1  SP  disk0:                       128577536     105621504       82%
         1  SP  sup-bootflash:                31981568      29700644       93%
         1  SP  const_nvram:                    129004           856        1%
         1  SP  nvram:                          391160         22065        6%
         7      dfc#7-bootflash:              15204352        616540        4%
         8      dfc#8-bootflash:              15204352             0        0%
Router#
```

This example shows how to display the capacity and utilization of the EARLs present in the system:

```
Router# show platform hardware capacity forwarding
L2 Forwarding Resources
           MAC Table usage:   Module  Collisions  Total       Used       %Used
                              6                0  65536         11          1%
             VPN CAM usage:                       Total       Used       %Used
                                                    512          0          0%
L3 Forwarding Resources
             FIB TCAM usage:                     Total        Used       %Used
                  72 bits (IPv4, MPLS, EoM)     196608          36          1%
                 144 bits (IP mcast, IPv6)       32768           7          1%
                     detail:      Protocol                    Used       %Used
                                  IPv4                          36          1%
                                  MPLS                           0          0%
                                  EoM                            0          0%
                                  IPv6                           4          1%
                                  IPv4 mcast                     3          1%
                                  IPv6 mcast                     0          0%
            Adjacency usage:                     Total        Used       %Used
```

```
                                            1048576        175          1%
     Forwarding engine load:
                     Module        pps   peak-pps                     peak-time
                     6               8       1972  02:02:17 UTC Thu Apr 21 2005
Netflow Resources
          TCAM utilization:       Module       Created      Failed       %Used
                                  6                  1           0          0%
          ICAM utilization:       Module       Created      Failed       %Used
                                  6                  0           0          0%
                 Flowmasks:   Mask#   Type        Features
                        IPv4:     0   reserved    none
                        IPv4:     1   Intf FulNAT_INGRESS NAT_EGRESS FM_GUARDIAN
                        IPv4:     2   unused      none
                        IPv4:     3   reserved    none
                        IPv6:     0   reserved    none
                        IPv6:     1   unused      none
                        IPv6:     2   unused      none
                        IPv6:     3   reserved    none
CPU Rate Limiters Resources
             Rate limiters:       Total         Used      Reserved       %Used
                    Layer 3           9            4             1         44%
                    Layer 2           4            2             2         50%
ACL/QoS TCAM Resources
  Key: ACLent - ACL TCAM entries, ACLmsk - ACL TCAM masks, AND - ANDOR,
       QoSent - QoS TCAM entries, QOSmsk - QoS TCAM masks, OR - ORAND,
       Lbl-in - ingress label, Lbl-eg - egress label, LOUsrc - LOU source,
       LOUdst - LOU destination, ADJ - ACL adjacency
  Module ACLent ACLmsk QoSent QoSmsk Lbl-in Lbl-eg LOUsrc LOUdst  AND  OR  ADJ
  6          1%     1%     1%     1%     1%     1%     0%     0%   0%  0%   1%
Router#
```

This example shows how to display the interboard communication resources:

```
Router# show platform hardware capacity ibc
IBC Resources
  Module                     Packets/sec     Total packets     Dropped packets
  1  RP      Rx:                       3           5001419                   0
             Tx:                       1           1943884                   0
Router#
```

This example shows how to display the interface resources:

```
Router# show platform hardware capacity interface
Interface Resources
  Interface drops:
    Module    Total drops:    Tx            Rx      Highest drop port:  Tx  Rx
    9                          0             2                           0  48
  Interface buffer sizes:
    Module                            Bytes:     Tx buffer           Rx buffer
         1                                           12345               12345
         5                                           12345               12345
Router#
```

This example shows how to display SPAN information:

```
Router# show platform hardware capacity monitor
SPAN Resources
  Source sessions: 2 maximum, 0 used
    Type                                 Used
    Local                                   0
    RSPAN source                            0
    ERSPAN source                           0
    Service module                          0
```

```
  Destination sessions: 64 maximum, 0 used
    Type                                    Used
    RSPAN destination                          0
    ERSPAN destination (max  24)               0
Router#
```

This example shows how to display the capacity and utilization of resources for Layer 3 multicast functionality:

```
Router# show platform hardware capacity
 multicast
L3 Multicast Resources
  IPv4 replication mode: ingress
  IPv6 replication mode: ingress
  Bi-directional PIM Designated Forwarder Table usage: 4 total, 0 (0%) used
  Replication capability: Module                              IPv4        IPv6
                          5                                 egress      egress
                          9                                ingress     ingress
  MET table Entries: Module                             Total    Used    %Used
                     5                                  65526       6       0%
Router#
```

This example shows how to display information about the system power capacities and utilizations:

```
Router# show platform hardware capacity power
Power Resources
  Power supply redundancy mode: administratively combined
                                                        operationally combined
  System power: 1922W, 0W (0%) inline, 1289W (67%) total allocated
  Powered devices: 0 total
Router#
```

This example shows how to display the capacity and utilization of QoS policer resources per EARL in the Cisco 7600 series router:

```
Router# show platform hardware capacity qos
 QoS Policer Resources
  Aggregate policers: Module                      Total         Used     %Used
                      1                            1024          102       10%
                      5                            1024            1        1%
  Microflow policer configurations: Module        Total         Used     %Used
                                    1                64           32       50%
                                    5                64            1        1%
Router#
```

This example shows how to display information about the key system resources:

```
Router# show platform hardware capacity system
System Resources
  PFC operating mode: PFC3BXL
  Supervisor redundancy mode: administratively rpr-plus, operationally rpr-plus
  Switching Resources: Module   Part number               Series      CEF mode
                       5        WS-SUP720-BASE        supervisor           CEF
                       9        WS-X6548-RJ-45            CEF256           CEF
Router#
```

This example shows how to display VLAN information:

```
Router# show platform hardware capacity vlan
VLAN Resources
```

```
  VLANs: 4094 total, 10 VTP, 0 extended, 0 internal, 4084 free
Router#
```

Related Commands

Command	Description
show msfc	Displays MSFC information.
show platform	Displays platform information.
show platform hardware capacity rewrite-engine	Displays the packet drop and performance counters of the central rewrite engine on supervisors and line cards.

show platform hardware capacity rewrite-engine

To display the packet drop and performance counters of the central rewrite engine on supervisors and line cards, use the **show platform hardware capacity rewrite-engine** command in privileged EXEC mode.

show platform hardware capacity rewrite-engine {**drop** | **performance**} [**slot** *number*] [**rate** [{*sample interval*}]][**details**]

Syntax Description

drop	Displays the central rewrite engine drop counter values.
performance	Displays the central rewrite engine current performance counter values or the performance rate.
slot *number*	(Optional) Displays the counter values for the module in the specified slot. If no slot is specified, the counters are displayed for each slot.
rate [*sample_interval*]	(Optional) Displays the drop rate or rewrite rate for a sample interval in msec between 1 and 1000. The default interval is 50 msec.
details	(Optional) Displays each individual drop counter with its name and register ID number. This keyword is not available with the **performance** keyword.

Command Default

If the sample interval is not specified, the default interval is 50 msec.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
15.1(1)S	Support was added for Cisco 7600 routers. This command replaces the **show platform hardware central-rewrite**command.

Usage Guidelines

In the output of the **show platform hardware capacity rewrite-engine performance** command output, a value of �N/A� means the slot/channel has a rewrite engine, but does not support performance counters.

Examples

The following sample output of the **show platform hardware capacity rewrite-engine drop**command displays the packet drop counters of the central rewrite engine in all installed supervisors and line cards:

```
Router# show platform hardware capacity rewrite-engine drop
slot channel   packet drops      total overruns
----+---------+-----------------+------------------+
1    0         0                 0
5    0         15440040          22
7    0         44                0
7    1         0                 0
```

Examples

The following sample output of the **show platform hardware capacity rewrite-engine drop**command displays the packet drop counters of the central rewrite engine in all installed supervisors and line cards:

```
Router# show platform hardware capacity rewrite-engine drop
slot channel   packet drops      total overruns
----+---------+-----------------+------------------+
1    0         0                 0
5    0         15440040          22
7    0         44                0
7    1         0                 0
```

The following sample output of the **show platform hardware capacity rewrite-engine drop**command displays a detailed report of the packet drop counters of the module in slot 1:

```
Router# show platform hardware capacity rewrite-engine drop slot 1 details
slot channel drop_id description          packet drops     total overruns
----+-------+-------+--------------------+----------------+--------------+
1    0       0x5ED   DROP NON BPDU        0                0
1    0       0x5EB   DROP BPDU            0                0
1    1       0x5ED   DROP NON BPDU        0                0
1    1       0x5EB   DROP BPDU            0                0
```

The following sample output of the **show platform hardware capacity rewrite-engine drop**command displays the packet drop counters of the module in slot 5 over the default sample interval of 50 msec:

```
Router# show platform hardware capacity rewrite-engine drop slot 5 rate
slot channel   drop rate [pps]        overrun [Y/N]
----+---------+----------------------+-------------+
5    0         120079                 Y
```

The following sample output of the **show platform hardware capacity rewrite-engine drop**command displays the packet drop counters of the module in slot 5 over a sample interval of 20 msec:

```
Router# show platform hardware capacity rewrite-engine drop slot 5 rate 20
slot channel   drop rate [pps]        overrun [Y/N]
----+---------+----------------------+-------------+
5    0         180000                 N
```

The following sample output of the **show platform hardware capacity rewrite-engine drop**command displays the performance counters of the central rewrite engine in all installed supervisors and line cards:

```
Router# show platform hardware capacity rewrite-engine performance
slot channel perf_id description          packets          total overruns
----+-------+-------+--------------------+----------------+--------------+
1    0       0x235   FAB RX 0             12870            0
1    0       0x237   FAB RX 1             0                0
1    0       0x27B   FAB TX 0             164              0
1    0       0x27F   FAB TX 1             0                0
1    0       0x350   REPLICATION ML3      0                0
1    0       0x351   REPLICATION ML2      0                0
1    0       0x352   RECIRC L2            0                0
1    0       0x353   RECIRC L3            0                0
1    0       0x34C   SPAN TX 0            0                0
1    0       0x34D   SPAN TX 1            0                0
1    0       0x34E   SPAN RX 0            0                0
1    0       0x34F   SPAN RX 1            0                0
1    0       0x354   SPAN TERMINATION     0                0
```

```
1    1       0x235   FAB RX 0             106065          0
1    1       0x237   FAB RX 1             0               0
1    1       0x27B   FAB TX 0             180806          0
1    1       0x27F   FAB TX 1             0               0
1    1       0x350   REPLICATION ML3      0               0
1    1       0x351   REPLICATION ML2      0               0
1    1       0x352   RECIRC L2            0               0
1    1       0x353   RECIRC L3            0               0
1    1       0x34C   SPAN TX 0            0               0
1    1       0x34D   SPAN TX 1            0               0
1    1       0x34E   SPAN RX 0            201             0
1    1       0x34F   SPAN RX 1            90201           0
1    1       0x354   SPAN TERMINATION     0               0
4    0       N/A
5    0       0xBE    FAB RX 0             181496          0
5    0       0xC0    FAB RX 1             0               0
5    0       0x112   FAB TX 0             992089          0
5    0       0x116   FAB TX 1             0               0
5    0       0x299   REPLICATION ML3      0               0
5    0       0x29A   REPLICATION ML2      0               0
5    0       0x29B   RECIRC L2            0               0
5    0       0x29C   RECIRC L3            0               0
5    0       0x295   SPAN TX 0            91166           0
5    0       0x296   SPAN TX 1            91313           0
5    0       0x297   SPAN RX 0            1               0
5    0       0x298   SPAN RX 1            1               0
5    0       0x29D   SPAN TERMINATION     0               0
```

The following sample output of the **show platform hardware capacity rewrite-engine drop**command displays the performance counters of the module in slot 5:

```
Router# show platform hardware capacity rewrite-engine performance slot 5
slot channel perf_id description          packets          total overruns
----+-------+-------+--------------------+----------------+--------------+
5    0       0xBE    FAB RX 0             1330            0
5    0       0xC0    FAB RX 1             0               0
5    0       0x112   FAB TX 0             715253          0
5    0       0x116   FAB TX 1             0               0
5    0       0x299   REPLICATION ML3      0               0
5    0       0x29A   REPLICATION ML2      0               0
5    0       0x29B   RECIRC L2            0               0
5    0       0x29C   RECIRC L3            0               0
5    0       0x295   SPAN TX 0            1022            0
5    0       0x296   SPAN TX 1            1152            0
5    0       0x297   SPAN RX 0            1               0
5    0       0x298   SPAN RX 1            1               0
5    0       0x29D   SPAN TERMINATION     0               0
```

The following sample output of the **show platform hardware capacity rewrite-engine drop**command displays the performance counters of the module in slot 5 over the default sample interval of 50 msec:

```
Router# show platform hardware capacity rewrite-engine performance slot 5 rate
slot channel perf_id description          packet rate[pps] overrun [Y/N]
----+-------+-------+--------------------+----------------+--------------+
5    0       0xBE    FAB RX 0             11680           N
5    0       0xC0    FAB RX 1             0               N
5    0       0x112   FAB TX 0             11680           N
5    0       0x116   FAB TX 1             0               N
5    0       0x299   REPLICATION ML3      0               N
5    0       0x29A   REPLICATION ML2      0               N
5    0       0x29B   RECIRC L2            0               N
5    0       0x29C   RECIRC L3            0               N
5    0       0x295   SPAN TX 0            5840            N
```

```
5    0       0x296   SPAN TX 1            5840             N
5    0       0x297   SPAN RX 0            0                N
5    0       0x298   SPAN RX 1            0                N
5    0       0x29D   SPAN TERMINATION     0                N
```

Related Commands

Command	Description
clear platform hardware capacity rewrite-engine counter	Clears the packet drop and performance counters of the central rewrite engine on supervisors and line cards.

show platform hardware interface

To display information about an interface, use the **showplatformhardwareinterface**command in privileged EXEC or diagnostic mode.

show platform hardware interface type number plim qos input map

Channelized T3 Shared Port Adapters
show platform hardware interface serial slot/subslot/port/t1-number:channel-group plim qos input map

Channelized T1/E1 Shared Port Adapters
show platform hardware interface serial slot/subslot/port:channel-group plim qos input map

Shared Port Adapters
show platform hardware interface type slot/subslot/port [.subint] plim qos input map

Syntax Description

type	Interface type. The table in the "Usage Guidelines" contains a list of interface types.
number	Port number on the selected interface.
plim qos input map	Physical Line Interface Module (PLIM) QoS input mapping information.
serial	Serial interface.
slot/subslot/port/t1-number:channel-group	The following applies to Channelized T3 shared port adapters: • slot/--Chassis slot where the Cisco ASR 1000 Series SPA interface processor (SIP) is installed. • subslot/--Secondary slot number of the SIP where the Cisco ASR 1000 Series shared port adapter (SPA) is installed. • port/--Interface number on the SPA. • t1-number--T1 time slot in the T3 line. The value can be from 1 to 28. • channel-group--Number 0 to 23 of the DS0 link on the T1 channel. **Note** When a port on a Channelized T3 SPA is configured to be in unchannelized mode, only the slot/subslot/port/ arguments are used to specify the unchannelized T3 interface. The t1-number and channel-group arguments are not used.

slot/subslot/port: channel-group	The following applies to Channelized T1/E1 shared port adapters: • slot/--Chassis slot where the Cisco ASR 1000 Series SPA interface processor (SIP) is installed. • subslot/--Secondary slot number of the SIP where the Cisco ASR 1000 Series shared port adapter (SPA) is installed. • port--Interface number on the SPA. • channel-group--Number 0 to 30 of the DS0 link on the T1 channel.
slot/subslot/port [.subint]	The following applies to shared port adapters other than the Channelized T3 or Channelized T1/E1 shared port adapters: • slot/--Chassis slot where the Cisco ASR 1000 Series SPA interface processor (SIP) is installed. • subslot/--Secondary slot number of the SIP where the Cisco ASR 1000 Series shared port adapter (SPA) is installed. • port--Interface number on the SPA. • (Optional) .subint--Subinterface number (for those SPAs that support subinterface configuration).

Command Default

No default behavior or values

Command Modes

Privileged EXEC (#)

Diagnostic (diag)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines

This command displays platform-specific information and configuration information related to a specific interface.

The table below lists the interface types.

Table 192: Interface Types

Interface Type	Description
async	Asynchronous interface
auto-template	Auto-template interface
bvi	Bridge group virtual interface
ctunnel	Connectionless Network Service (CLNS) tunnel (CTunnel) interface
container	Container interface

Interface Type	Description
dialer	Dialer interface
esconphy	ESCON interface
fastethernet	Fast Ethernet IEEE 802.3 interface
filter	Filter interface
filtergroup	Filter group interface
gigabitethernet	Gigabit Ethernet IEEE 802.3 interface.
group-async	Group asynchronous interface
lex	LAN extender (LEX) interface
longreachethernet	Long Reach Ethernet interface
loopback	Loopback interface
multilink	Multilink group interface
null	Null interface
pos	Packet over SONET (POS) interface
port-channel	Ethernet channel of interfaces
portgroup	Port group interface
pos-channel	POS channel of interfaces
sbc	Session border controller interface
sysclock	Telecom bus clock controller interface
serial	Serial interface
tunnel	Tunnel interface
vif	Pragmatic General Multicast (PGM) host interface
virtual-ppp	Virtual point-to-point (PPP) interface
virtual-template	Virtual template interface
virtual-tokenring	Virtual Token Ring interface
vlan	Catalyst VLAN interface
fcpa	Fiber Channel interface
multiservice	Multiservice interface
voabyapssin	Variable optical attenuator (VOA) bypass-in interface

Interface Type	Description
voabyapssout	VOA bypass-out interface
voafilterin	VOA filter-in interface
voafilterout	VOA filter-out interface
voain	VOA-in interface
voaout	VOA-out interface

Examples

Packets can be classified based on the IP precedence, IPv6 traffic class, MPLS experimental bits, or VLAN TOS bits. In the following example, incoming packets with IP precedence 6 or 7, IPv6 packets with traffic class 46, and MPLS packets with experimental bits 6 or 7 are classified as high priority packets:

```
Router# show platform hardware interface gigabitethernet 0/0/0 plim qos input map
Interface GigabitEthernet0/0/0
Low Latency Queue(High Priority):
IP PREC, 6, 7
IPv6 TC, 46
MPLS EXP, 6, 7
```

Related Commands

Command	Description
show platform hardware port	Displays information about an interface port on a shared port adapter (SPA).
show platform hardware slot	Displays information about the processor in a chassis slot.
show platform hardware subslot	Displays information about a shared port adapter (SPA).

show platform hardware network-clocks

To display network clocks for an ES+ line card, use the **showplatformhardwarenetwork-clocks**command in privileged EXEC mode.

show platform hardware network-clocks [{**bits** | **zl30138**}]

Syntax Description

bits	Specifies uilding Integrated Timing Supply (BITS) element.
zl30138	Specifies ZL30138 SONET/SDH/10GbE System Synchronizer.
sec GNSS	Displays the standby GNSS module device information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRD1	This command was introduced on the Cisco 7600 series routers for ES+ line cards only.

Examples

The following example shows how the **showplatformhardwarenetwork-clocks**command is used to display network clocks:

```
Router# show platform hardware network-clocks

Local Loop Timing:

    Port 1: N    Port 2: N    Port 3: N    Port 4: N

Backplane Bus Status and Source:

    Primary   : Disabled, Port 0 RX_DEMAP Clock
    Secondary : Disabled, Port 0 RX_DEMAP Clock
    BITS      : Disabled, Port 0 RX_DEMAP Clock

ZL30138 Configuration and Status:

    DPLL1: Failure (4)
        Mode of Operation  : Manual Freerun
        Selected Reference : 0
        Ref0 Priority : 15        Ref1 Priority : 15
        Ref2 Priority : 15        Ref3 Priority : 15
        Ref4 Priority : 15        Ref5 Priority : 15
        Ref6 Priority : 15        Ref7 Priority : 15

    Reference Monitoring: Custom A frequency 25000 kHz
        Ref#    SCM    CFM    GST    PFM    Mode      Detected
        ----------------------------------------------------------
        0       1      1      1      1      CustA     38.88 MHz
        1       1      1      1      1      CustA     19.44 MHz
        2       0      0      0      0      Auto      77.76 MHz
        3       1      1      1      1      CustA     not detected
        4       1      1      1      1      Auto      not detected
```

```
        5       1       1       1       1       Auto      not detected
        6       1       1       1       1       Auto      not detected
        7       1       1       1       1       Auto      not detected

BITS Configuration and Status:

    Signal Type   : T1 ESF Framing
    Clock Divider : 1.544 MHz


Router# show platform hardware network-clocks | sec GNSS
GNSS status
  GNSS device: not detected
  Lock status: Disabled
  Survey progress: 0
  Satelite count: 0
  Firmware version: 0.0
  Firmware update progress: NA
  GNSS TAM Authentication: Not applicable
  Serial number:
```

Related Commands

Command	Description
clock source	Specifies the interface clock source type.
network-clock select	Selects a source of network clock.
show network-clocks	Displays the current configured and active network clock sources.

show platform hardware pp active interface all

Use this command to verify the bandwidth and port speed.

show platform hardware pp active interface all

There are no keywords for this command.

Command Default

None

Command Modes

Privileged EXEC

Examples

The following example shows how to verify the bandwidth and port speed:

```
Router#show platform hardware pp active interface all
Interface manager platform keys
-------------------------------------------------
Name: TenGigabitEthernet0/4/7, Asic: 0, hwidx: 9
lpn: 0, ppn: 9, gid: 9, mac: c8f9.f98d.202b
InLportId: 0, ELportId: 0, dpidx: 31, l3ID: 25
port_flags: 0, port_speed: 10000 Mbps, efp_count: 0, destIndex: 9, intType: 1
etherchnl: 0, efp: 0, bdi: 0, l2PhyIf: 0, l3PhyIf: 1, l3TDM: 0, loopBack: 0
tunnel: 0, tunneltp: 0, icmp_flags: 0, icmp6_flags: 0
bandwidth: 10000000, fcid: 0, cid: 0, mpls_tbid: 0, protocols: 4
v4_netsmask: 8, v4_tableid: 8, v6_tableid: 65535, vrf_tbid_dstrm: , snmp_index: 0
bd_id: 0, encap: 1, ip_mtu: 1500, l2_max_tu: 1500, l2_min_tu: 0
vrfid: 8, enctype: 0, admin_state: 1, admin_state_oir: 0
Name: TenGigabitEthernet0/4/6, Asic: 0, hwidx: 10
lpn: 0, ppn: 10, gid: 10, mac: c8f9.f98d.202a
InLportId: 0, ELportId: 0, dpidx: 30, l3ID: 24
port_flags: 0, port_speed: 10000 Mbps, efp_count: 0, destIndex: 10, intType: 1
etherchnl: 0, efp: 0, bdi: 0, l2PhyIf: 0, l3PhyIf: 1, l3TDM: 0, loopBack: 0
tunnel: 0, tunneltp: 0, icmp_flags: 0, icmp6_flags: 0
bandwidth: 10000000, fcid: 0, cid: 0, mpls_tbid: 0, protocols: 4
v4_netsmask: 8, v4_tableid: 6, v6_tableid: 65535, vrf_tbid_dstrm: , snmp_index: 0
bd_id: 0, encap: 1, ip_mtu: 1500, l2_max_tu: 1500, l2_min_tu: 0
vrfid: 6, enctype: 0, admin_state: 1, admin_state_oir: 0
```

Related Commands

Command	Description
hw-module subslot *slot* / *subslot* **ether-mode 10G**	Configures the 10G mode from 1G mode.
hw-module subslot *slot* / *subslot* **ether-mode 1G**	Configures the 1G mode from 10G mode.

show platform hardware qfp active feature cef-mpls urpf

To confirm and display the hardware information pertaining to Cisco Express Forwarding (CEF) Multiprotocol Label Switching (MPLS) Unicast Reverse Path Forwarding (uRPF) feature on a Cisco QuantumFlow Processor (QFP) of the Cisco ASR 1000 Series Aggregation Services Routers, use the **show platform hardware qfp active feature cef-mpls urpf** command in privileged EXEC mode.

show platform hardware qfp active feature cef-mpls urpf *interface-name ip-version ip version*

Syntax Description

ip-version	Name of the interface.
interface-name	Version of the IP. Valid values are IPv4 and IPv6.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.0S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following is a sample output of the **show platform hardware qfp active feature cef-mpls urpf** command:

```
Device# show platform hardware qfp active feature cef-mpls urpf GigabitEthernet 0/0/0.777
ipv4


=== uRPF Information ===
  uRPF mode: Strict
  allow_default_route: FALSE
  allow_self_ping: FALSE
```

Related Commands

The table below describes the significant fields shown in the display.

Table 193: show platform hardware qfp active feature cef-mpls urpf Field Descriptions

Field	Description
uRPF mode	Mode of uRPF. Valid values are Strict or Loose..
allow_default_route	State showing whether the QFP allows the use of the default route in the source verification process or not. Valid values are TRUE or FALSE.
allow_self_ping	State showing whether the QFP allows the source of the packet to ping itself during the source verification process or not. Valid values are TRUE or FALSE.

show platform hardware qfp active feature cef-mpls prefix ip

To display the interface name along with the interface descriptor block (IDB) information, use the **showplatformhardwareqfpactivefeaturecef-mplsprefixip** command in privileged EXEC.

show platform hardware qfp active feature cef-mpls prefix ip {*ipv4 prefix* | [**vrf** [{*id*}]] [**exact**] [**brief**]}

Syntax Description

ipv4 prefix	IPv4 address and mask.
vrf	(Optional) Displays information about VPN Routing and Forwarding (VRF).
id	(Optional) Information about the particular VRF instance. The range is from 0 to 4294967295. If no VRF ID is specified, information about the global VRF, which is the prefix in global routing table, is displayed.
exact	(Optional) Find and displays the exact match of the IPV4 prefix.
brief	(Optional) Displays a summary of prefix information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)XNB	This command was introduced on the Cisco ASR 1000 Series Routers.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS Release XE 3.4S. Support for IP Fast Reroute (IP FRR) was added.

Examples

The following is sample output from the**showplatformhardwareqfpactivefeaturecef-mplsprefixip** command:

```
Router# show platform hardware qfp active feature cef-mpls prefix ip 0.0.0.0/1 vrf
Gtrie Node Type: Leaf Node
HW Content: : 00002000 00000000 897daf40 895db490
  QPPB QoS Precedence valid: 0
  QoS Precedence: 0
  QPPB QoS Group valid: 0
  QoS Group: 0
  BGPPA Traffic Index valid: 0
  BGPPA Traffic Index: 0
  TBLF refcount: 2
  TBLF application lf handle: 0
  Prefix Length: 32
  Prefix: 64 00 00 01
=== uRPF path list ===
  Loose Flag: : 1
  Path list pointer: : 0x8b8414a0
  Number of interfaces: : 1
  Interfaces: : 1017
  Interface Name(s): GigabitEthernet0/3/1
=== OCE ===
OCE Type: Adjacency, Number of children: 0
```

```
Adj Type: : IPV4 Adjacency
Encap Len: : 14
L3 MTU: : 1500
Adj Flags: : 0
Fixup Flags: : 0
Output UIDB: : 65522
Interface Name: GigabitEthernet0/3/1
Encap: : 00 14 f1 74 9c 1a 00 1a 30 44 3a 31 08 00
Next Hop Address: : 64000001 00000000 00000000 00000000
Oce Chain: : 0
```

The following example shows the output with the names of each interface when there are multiple interfaces in the unicast reverse path forwarding (uRPF) path list:

Router# **show platform hardware qfp active feature cef-mpls prefix ip 0.0.0.0/2 vrf**

```
Gtrie Node Type: Leaf Node
HW Content: : 00001800 00000000 897dae00 895d8df0
  QPPB QoS Precedence valid: 0
  QoS Precedence: 0
  QPPB QoS Group valid: 0
  QoS Group: 0
  BGPPA Traffic Index valid: 0
  BGPPA Traffic Index: 0
  TBLF refcount: 2
  TBLF application lf handle: 0
  Prefix Length: 24
  Prefix: 4d 4d 4d
=== uRPF path list ===
  Loose Flag: : 1
  Path list pointer: : 0x8b8414a0
  Number of interfaces: : 2
  Interfaces: : 1019, 1017
  Interface Name(s): : GigabitEthernet0/0/4, GigabitEthernet0/3/1
```

show platform hardware qfp active feature cef-mpls prefix mpls

To display the complete Output Chain Element (OCE) chains used for handling the incoming Multiprotocol Label Switching (MPLS) packets with a particular label, use the show platform hardware qfp active feature cef-mpls prefix mpls command in the privileged EXEC mode.

show platform hardware qfp active feature cef-mpls prefix mpls mpls-label exact

Syntax Description

mpls-label	MPLS label containing a 20-bit label value, a 3-bit experimental field, a 1-bit bottom-of-stack indicator, and an 8-bit Time-to-Live (TTL) field.
exact	Displays all the OCE chains that are used for handling the incoming MPLS packets with a particular label.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following is sample output from the show platform hardware qfp active feature cef-mpls prefix mpls mpls-label exact command displaying all the OCE chains used for handling incoming MPLS packets with a particular label:

```
Router# show platform hardware qfp active feature cef-mpls prefix mpls 17 exact
Gtrie Node Type: Leaf Node
HW Content: : 0a000000 00000f00 00000000 8bb08a30
QPPB QoS Precedence valid: 0
QoS Precedence: 0
QPPB QoS Group valid: 0
QoS Group: 0
BGPPA Traffic Index valid: 0
BGPPA Traffic Index: 0
TBLF refcount: 2
TBLF application lf handle: 0
CTS src_sgt: 0
CTS dst_sgt: 0
Prefix Length: 20
Prefix: 00 0d 00
Lisp local eid: 0
Lisp remote eid: 0
Lisp locator status bits: 0
Lisp dynamic configured eid: 0
Lisp dynamic discovered eid: 0
OCE Type: EOS OCE, Number of children: 2
Next HW OCE Ptr: : 0x8bb07e10, 0x8bb07e00
OCE Type: REPLICATE OCE, Number of children: 2
Replica_node: : 0x8ca90a20
Next HW OCE Ptr: : 0x8bb07eb0, 0x8bb08840
OCE Type: Label OCE, Number of children: 1
Label flags: : 64
Num Labels: : 1
```

```
Num Bk Labels: : 0
Out Labels: : 1048577
Next HW OCE Ptr: : 0x8bb07e60
OCE Type: Interface OCE, Number of children: 1
Next HW OCE Ptr: : 0x8bb07e40
Interface Name: Lspvif20
OCE Type: Lookup OCE, Number of children: 0
Lookup flags: : 1
Table Type: : 0
Lookup table ID: : 0
OCE Type: Label OCE, Number of children: 1
Label flags: : 0
Num Labels: : 1
Num Bk Labels: : 1
Out Labels: : 88
Out Backup Labels: : 0
Next HW OCE Ptr: : 0x8bb06ca0
OCE Type: Adjacency, Number of children: 0
Adj Type: : MPLS Adjacency
Encap Len: : 14
L3 MTU: : 1500
Adj Flags: : 0
Fixup Flags: : 0
Interface Name: GigabitEthernet0/1/0
Encap: : 00 0e 39 88 70 19 00 21 d8 60 c0 10 88 47
Next Hop Address: : 0f000001 00000000 00000000 00000000
Next HW OCE Ptr: : 00000000
OCE Type: REPLICATE OCE, Number of children: 2
Replica_node: : 0x8ca90a00
Next HW OCE Ptr: : 0x8bb07e70, 0x8bb08840
OCE Type: Label OCE, Number of children: 1
Label flags: : 64
Num Labels: : 1
Num Bk Labels: : 0
Out Labels: : 1048577
Next HW OCE Ptr: : 0x8bb07e50
OCE Type: Interface OCE, Number of children: 1
Next HW OCE Ptr: : 0x8bb001f0
Interface Name: Lspvif20
OCE Type: Lookup OCE, Number of children: 0
Lookup flags: : 0
Table Type: : 1
Lookup table ID: : 2
OCE Type: Label OCE, Number of children: 1
Label flags: : 0
Num Labels: : 1
Num Bk Labels: : 1
Out Labels: : 88
Out Backup Labels: : 0
Next HW OCE Ptr: : 0x8bb06ca0
OCE Type: Adjacency, Number of children: 0
Adj Type: : MPLS Adjacency
Encap Len: : 14
L3 MTU: : 1500
Adj Flags: : 0
Fixup Flags: : 0
Interface Name: GigabitEthernet0/1/0
Encap: : 00 0e 39 88 70 19 00 21 d8 60 c0 10 88 47
Next Hop Address: : 0f000001 00000000 00000000 00000000
Next HW OCE Ptr: : 00000000
The fields shown in the display are self-explanatory.
```

show platform hardware qfp active feature multicast

To display the complete Output Chain Element (OCE) chains that are connected by each leaf node in the multicast replication tree for a particular output path in the Cisco QuantumFlow Processor (QFP) active feature on the Cisco ASR 1000 Series Aggregation Services Routers, use the show platform hardware qfp active feature multicast command in the privileged EXEC mode.

show platform hardware qfp active feature multicast ip-version ip-address-mgroup [**ip-address-source**] **vrf vrf-id extension**

Syntax Description

ip-version	Version of the IP address. It can be one of the following values: • v4mcast—IPv4. • v6mcast—IPv6.
ip-address-mgroup	Multicast group's IP address.
ip-address-source	(Optional) Source prefix for the IP address.
vrf	Displays information present in a particular VRF.
vrf-id	ID of the VRF.
extension	Displays the entire OCE that is connected by each leaf node in the multicast replication tree for a particular output path.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following is sample output from the show platform hardware qfp active feature multicast v4mcast command displaying all the OCE chains used for forwarding traffic to a particular IPv4 multicast address:

```
Router# show platform hardware qfp active feature multicast v4mcast 239.1.1.1/32 vrf 2
extension
Root: 0x1187fc58
Flags: 0x000002
First leaf: 0x11887fa8
Number of nodes: 1
Number of leaves: 3
RPF i/f: 0x01fff7
Punt limit counter: 200
NS DCS Punt limit: 0x000001
RPF Fast Convergence Flags: 00000000
Secondary RPF interface: 00000000
RPF Fast Convergence Timer: 0
Extended leaf address: 0x89f80060
Node: 0x1187fc58
```

```
Cumulative Free Space: : 4
Cumulative Weight: : 3
Number of Children: : 3
Hw Addr: : 0x8b969440
Node Flags: : 0x000004
Software Child Ptr: : 0x1187fce0, 0x1187fd60, 0x11887fa8, 00000000
00000000, 00000000, 00000000
Hardware Child Ptr: : 0x89f8e440, 0x89f8e450, 0x89f8e460, 00000000
00000000, 00000000, 00000000
OCE Flags: : 0x000009
SW OCE chain ptr: 0x11884b48
HW OCE chain ptr: 0x895d59a0
OCE Type: Adjacency, Number of children: 1
Adj Type: : IPV4 Adjacency
Encap Len: : 0
L3 MTU: : 9216
Adj Flags: : 64
Fixup Flags: : 0
Interface Name: Lspvif0
Next Hop Address: : 00000000 00000000 00000000 00000000
Lisp locator status: : 00000000
Next HW OCE Ptr: : 0x895d5940
OCE Type: REPLICATE OCE, Number of children: 1
Replica_node: : 0x89fab440
Next HW OCE Ptr: : 0x895d5ab0
OCE Type: Label OCE, Number of children: 1
Label flags: : 0
Num Labels: : 1
Num Bk Labels: : 1
Out Labels: : 17
Out Backup Labels: : 0
Next HW OCE Ptr: : 0x895d5a70
OCE Type: Label OCE, Number of children: 1
Label flags: : 65
Num Labels: : 1
Num Bk Labels: : 0
Out Labels: : 3
Next HW OCE Ptr: : 0x895d59f0
OCE Type: Adjacency, Number of children: 0
Adj Type: : MPLS Adjacency
Encap Len: : 14
L3 MTU: : 1500
Adj Flags: : 0
Fixup Flags: : 0
Interface Name: GigabitEthernet0/1/0
Encap: : 00 24 14 f4 9d 00 00 21 d8 d4 a5 10 88 47
Next Hop Address: : 0b000002 00000000 00000000 00000000
Next HW OCE Ptr: : 00000000
OCE Flags: : 0x000002
SW OCE chain ptr: 0x118830d0
HW OCE chain ptr: 0x895d58f0
OCE Type: Adjacency, Number of children: 0
Adj Type: : IPV4 Adjacency
Encap Len: : 20
L3 MTU: : 1480
Adj Flags: : 0
Fixup Flags: : 2
Interface Name: Tunnel1
Encap: : 45 00 00 00 00 00 00 00 ff 67 39 94 c0 00 01 01
c0 00 01 01
Next Hop Address: : 00000000 00000000 00000000 00000000
Lisp locator status: : 00000000
Next HW OCE Ptr: : 00000000
OCE Flags: : 0x000009
```

```
SW OCE chain ptr: 0x1186c250
HW OCE chain ptr: 0x895d5650
OCE Type: Adjacency, Number of children: 0
Adj Type: : IPV4 Adjacency
Encap Len: : 14
L3 MTU: : 1500
Adj Flags: : 0
Fixup Flags: : 64
Interface Name: GigabitEthernet0/1/2
Encap: : 01 00 5e 00 00 00 00 21 d8 d4 a5 12 08 00
Next Hop Address: : e1000000 00000000 00000000 00000000
Lisp locator status: : 00000000
Next HW OCE Ptr: : 00000000
OCE Flags: : 0x000009
SW OCE chain ptr: 0x1186d478
HW OCE chain ptr: 0x895d5660
OCE Type: Adjacency, Number of children: 0
Adj Type: : IPV4 Adjacency
Encap Len: : 14
L3 MTU: : 1500
Adj Flags: : 0
Fixup Flags: : 64
Interface Name: GigabitEthernet0/1/4
Encap: : 01 00 5e 00 00 00 00 21 d8 d4 a5 14 08 00
Next Hop Address: : e1000000 00000000 00000000 00000000
Lisp locator status: : 00000000
Next HW OCE Ptr: : 00000000
```

The fields shown in the display are self-explanatory.

The following is sample output from the show platform hardware qfp active feature multicast v6mcast command displaying all the OCE chains used for forwarding traffic to a particular IPv6 multicast address:

```
Router# show platform hardware qfp active feature multicast v6mcast FF04::10/128 vrf 503316482
 extension
Root: 0x11b6c700
Flags: 0x000002
First leaf: 0x11e55bc8
Number of nodes: 1
Number of leaves: 3
RPF i/f: 0x01fff3
Punt limit counter: 200
NS DCS Punt limit: 0x000001
RPF Fast Convergence Flags: 00000000
Secondary RPF interface: 00000000
RPF Fast Convergence Timer: 0
Extended leaf address: 0x8ba18c90
Node: 0x11b6c700
Cumulative Free Space: : 4
Cumulative Weight: : 3
Number of Children: : 3
Hw Addr: : 0x8ba06c60
Node Flags: : 0x000004
Software Child Ptr: : 0x11b6dcb0, 0x11b6e0b0, 0x11e55bc8, 00000000
00000000, 00000000, 00000000
Hardware Child Ptr: : 0x8ba24060, 0x8ba24070, 0x8ba245f0, 00000000
00000000, 00000000, 00000000
OCE Flags: : 0x000009
SW OCE chain ptr: 0x11b71af0
HW OCE chain ptr: 0x895ffa40
OCE Type: Adjacency, Number of children: 1
Adj Type: : IPV6 Adjacency
```

```
Encap Len: : 0
L3 MTU: : 9216
Adj Flags: : 64
Fixup Flags: : 0
Interface Name: Lspvif0
Next Hop Address: : 00000000 00000000 00000000 00000000
Lisp locator status: : 00000000
Next HW OCE Ptr: : 0x895ffa20
OCE Type: Label OCE, Number of children: 1
Label flags: : 0
Num Labels: : 1
Num Bk Labels: : 1
Out Labels: : 2
Out Backup Labels: : 2
Next HW OCE Ptr: : 0x895ff9f0
OCE Type: Adjacency, Number of children: 1
Adj Type: : MPLS Adjacency
Encap Len: : 0
L3 MTU: : 9216
Adj Flags: : 64
Fixup Flags: : 0
Interface Name: Lspvif0
Next Hop Address: : 00000000 00000000 00000000 00000000
Next HW OCE Ptr: : 0x895ff980
OCE Type: REPLICATE OCE, Number of children: 1
Replica_node: : 0x8ba51060
Next HW OCE Ptr: : 0x895ffa60
OCE Type: Label OCE, Number of children: 1
Label flags: : 0
Num Labels: : 1
Num Bk Labels: : 1
Out Labels: : 17
Out Backup Labels: : 0
Next HW OCE Ptr: : 0x895ff7b0
OCE Type: Adjacency, Number of children: 0
Adj Type: : MPLS Adjacency
Encap Len: : 14
L3 MTU: : 1500
Adj Flags: : 0
Fixup Flags: : 0
Interface Name: GigabitEthernet0/1/0
Encap: : 00 24 14 f4 9d 00 00 21 d8 d4 a5 10 88 47
Next Hop Address: : 0b000002 00000000 00000000 00000000
Next HW OCE Ptr: : 00000000
OCE Flags: : 0x000009
SW OCE chain ptr: 0x11b6b800
HW OCE chain ptr: 0x895ff6a0
OCE Type: Adjacency, Number of children: 0
Adj Type: : IPV6 Adjacency
Encap Len: : 14
L3 MTU: : 1500
Adj Flags: : 0
Fixup Flags: : 64
Interface Name: GigabitEthernet0/1/2
Encap: : 33 33 00 00 00 00 00 21 d8 d4 a5 12 86 dd
Next Hop Address: : ff0e0000 00000000 00000000 00000000
Lisp locator status: : 00000000
Next HW OCE Ptr: : 00000000
OCE Flags: : 0x000009
SW OCE chain ptr: 0x11b6ba08
HW OCE chain ptr: 0x895ff6e0
OCE Type: Adjacency, Number of children: 0
Adj Type: : IPV6 Adjacency
Encap Len: : 14
```

```
L3 MTU: : 1500
Adj Flags: : 0
Fixup Flags: : 64
Interface Name: GigabitEthernet0/1/4
Encap: : 33 33 00 00 00 00 00 21 d8 d4 a5 14 86 dd
Next Hop Address: : ff0e0000 00000000 00000000 00000000
Lisp locator status: : 00000000
Next HW OCE Ptr: : 00000000
OCE Flags: : 0x00000a
SW OCE chain ptr: 0x11b6de20
HW OCE chain ptr: 0x895ff770
OCE Type: Adjacency, Number of children: 0
Adj Type: : IPV6 Adjacency
Encap Len: : 4
L3 MTU: : 1460
Adj Flags: : 2
Fixup Flags: : 2
Interface Name: Tunnel5
Encap: : f8 00 01 47
Next Hop Address: : 00000000 00000000 00000000 00000000
Lisp locator status: : 00000000
Next HW OCE Ptr: : 00000000
Root: 0x11e4f428
Flags: 00000000
First leaf: 0x11e51b90
Number of nodes: 1
Number of leaves: 3
RPF i/f: 0x0003fd
Punt limit counter: 200
NS DCS Punt limit: 0x000001
RPF Fast Convergence Flags: 00000000
Secondary RPF interface: 00000000
RPF Fast Convergence Timer: 0
Extended leaf address: 0x8ba21210
Node: 0x11e4f428
Cumulative Free Space: : 4
Cumulative Weight: : 3
Number of Children: : 3
Hw Addr: : 0x8ba0c560
Node Flags: : 0x000004
Software Child Ptr: : 0x11e424b8, 0x11e332b8, 0x11e51b90, 00000000
Root: 0x11e50f20
Flags: 00000000
First leaf: 0x11e51b90
Number of nodes: 1
Number of leaves: 3
RPF i/f: 0x0003fd
Punt limit counter: 200
NS DCS Punt limit: 0x000001
RPF Fast Convergence Flags: 00000000
Secondary RPF interface: 00000000
RPF Fast Convergence Timer: 0
Extended leaf address: 0x8ba212a0
Node: 0x11e50f20
Cumulative Free Space: : 4
Cumulative Weight: : 3
Number of Children: : 3
Hw Addr: : 0x8ba0c560
Node Flags: : 0x000004
Software Child Ptr: : 0x11e424b8, 0x11e56f98, 0x11e51b90, 00000000
00000000, 00000000, 00000000
Hardware Child Ptr: : 0x8ba247a0, 0x8ba24750, 0x8ba24740, 00000000
00000000, 00000000, 00000000
OCE Flags: : 0x000009
```

```
SW OCE chain ptr: 0x11b6ba08
HW OCE chain ptr: 0x895ff6e0
OCE Type: Adjacency, Number of children: 0
Adj Type: : IPV6 Adjacency
Encap Len: : 14
L3 MTU: : 1500
Adj Flags: : 0
Fixup Flags: : 64
Interface Name: GigabitEthernet0/1/4
Encap: : 33 33 00 00 00 00 00 21 d8 d4 a5 14 86 dd
Next Hop Address: : ff0e0000 00000000 00000000 00000000
Lisp locator status: : 00000000
Next HW OCE Ptr: : 00000000
OCE Flags: : 0x000009
SW OCE chain ptr: 0x11b71af0
HW OCE chain ptr: 0x895ffa40
OCE Type: Adjacency, Number of children: 1
Adj Type: : IPV6 Adjacency
Encap Len: : 0
L3 MTU: : 9216
Adj Flags: : 64
Fixup Flags: : 0
Interface Name: Lspvif0
Next Hop Address: : 00000000 00000000 00000000 00000000
Lisp locator status: : 00000000
Next HW OCE Ptr: : 0x895ffa20
OCE Type: Label OCE, Number of children: 1
Label flags: : 0
Num Labels: : 1
Num Bk Labels: : 1
Out Labels: : 2
Out Backup Labels: : 2
Next HW OCE Ptr: : 0x895ff9f0
OCE Type: Adjacency, Number of children: 1
Adj Type: : MPLS Adjacency
Encap Len: : 0
L3 MTU: : 9216
Adj Flags: : 64
Fixup Flags: : 0
Interface Name: Lspvif0
Next Hop Address: : 00000000 00000000 00000000 00000000
Next HW OCE Ptr: : 0x895ff980
OCE Type: REPLICATE OCE, Number of children: 1
Replica_node: : 0x8ba51060
Next HW OCE Ptr: : 0x895ffa60
OCE Type: Label OCE, Number of children: 1
Label flags: : 0
Num Labels: : 1
Num Bk Labels: : 1
Out Labels: : 17
Out Backup Labels: : 0
Next HW OCE Ptr: : 0x895ff7b0
OCE Type: Adjacency, Number of children: 0
Adj Type: : MPLS Adjacency
Encap Len: : 14
L3 MTU: : 1500
Adj Flags: : 0
Fixup Flags: : 0
Interface Name: GigabitEthernet0/1/0
Encap: : 00 24 14 f4 9d 00 00 21 d8 d4 a5 10 88 47
Next Hop Address: : 0b000002 00000000 00000000 00000000
Next HW OCE Ptr: : 00000000
OCE Flags: : 0x000003
SW OCE chain ptr: 0x11b6b800
```

```
HW OCE chain ptr: 0x895ff6a0
OCE Type: Adjacency, Number of children: 0
Adj Type: : IPV6 Adjacency
Encap Len: : 14
L3 MTU: : 1500
Adj Flags: : 0
Fixup Flags: : 64
Interface Name: GigabitEthernet0/1/2
Encap: : 33 33 00 00 00 00 00 21 d8 d4 a5 12 86 dd
Next Hop Address: : ff0e0000 00000000 00000000 00000000
Lisp locator status: : 00000000
Next HW OCE Ptr: : 00000000
The fields shown in the display are self-explanatory.
```

show platform hardware qfp active infrastructure punt

To display the hardware and infrastructure information for punt statistics and configuration in an active instance of the Cisco Quantum Flow Processor (QFP), use the **show platform hardware qfp active infrastructure punt** command in privileged EXEC mode.

show platform hardware qfp active infrastructure punt [**config** | **internal-interface** | **policer** | **statistics** **{ interface** |**qfp** |**type** [**global-drop** | **inject-drop** | **per-cause** | **punt-drop**] }]

Syntax Description

config	Specifies the entries in the punt table.
internal-interface	Specifies the configuration for an internal interface.
policer	Specifies the punt policer configuration.
statistics	Specifies the punt statistics.
interface	Specifies the punt statistics for an interface.
qfp	Specifies the punt statistics for a specific qfp.
type	Specifies the aggregate statistics.
global-drop	Specifies the aggregate drop statistics.
inject-drop	Specifies the aggregate inject drop statistics.
per-cause	Specifies the aggregate per cause punt statistics.
punt-drop	Specifies the aggregate punt drop statistics.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 3.2.0S	This command was introduced.
Cisco IOS XE 3.13.0S	This command was integrated into Cisco IOS XE Release 3.13.0S.

Example

The following is sample output of the **show platform hardware qfp active infrastructure punt config** command:

```
Router# show platform hardware qfp active infrastructure punt config
Punt table base addr : 0x89C91010
  punt cause index     96
  punt cause name      VLAN Auto Sense FSOL
  maximum instances    1
  punt table address : 0x89C91190
  instance[0] ptr    : 0x89C919A0
    QFP interface handle : 2
```

```
    Interface name       : internal0/0/rp:0
   instance address        : 0x89C919A0
    fast failover address   : 0x89C8EC94
    Low priority policer    : 128
    High priority policer   : 129
```

The following table describes the significant fields shown in the display.

Table 194: show platform hardware qfp active infrastructure punt config Field Descriptions

Field	Description
Punt table base addr	Base address of the punt table.
punt cause index	Index number of the punt cause
punt cause name	Name of the punt cause.
maximum instances	The number of instances.
punt table address	Address of the punt table.
instance[0] ptr	Address where the packets are stored for each of the punt cause.
QFP interface handle	The handle number of the qfp interface.
Interface name	Name of the interface.
instance address	Points to the address for each instance.
fast failover address	Points to the address for a fast failover.
Low priority policer	Low priority policer number.
High priority policer	High priority policer number.

Example

The following is sample output of the **show platform hardware qfp a infrastructure punt policer** command:

```
Router# show platform hardware qfp active infrastructure punt policer
QFP Punt Policer Config Summary


Policer  Rate      PeakRate   ConformBurst  ExceedBurst   Scaling
Handle   (pps)     (pps)      (pps)         (pps)         Factor
---------------------------------------------------------------------
001      146484    0          2288          2288          0
002      4000      0          4000          0             0
003      3000      0          3000          0             0
004      40000     0          40000         0             0
```

The following table describes the significant fields shown in the display.

Table 195: show platform hardware qfp a infrastructure punt config Field Descriptions

Field	Description
Policer Handle	Indicates the number of the policer handle.
Rate	Indicates the configured rate in packets per second (pps).
Peak Rate	Indicates the peak rate in pps.
Conform Burst	Displays the number of packets marked as conforming to a specified rate.
Exceed Burst	Displays the number of packets marked as exceeding a specified rate.
Scaling Factor	Indicates the scaling factor.

Example

The following is sample output of the **show platform hardware qfp active infrastructure statistics type per-cause** command. The fields in the display are self-explanatory.

```
Router# show platform hardware qfp active infrastructure punt statistics type per-cause

Global Per Cause Statistics

  Number of punt causes =   97

  Per Punt Cause Statistics
                                                       Packets          Packets
  Counter ID  Punt Cause Name                          Received         Transmitted
  -------------------------------------------------------------------------------------
  000         Reserved                                 0                0
  001         MPLS ICMP Can't Fragment                 0                0
  002         IPv4 Options                             0                0
  003         Layer2 control and legacy                0                0
…
```

Example

The following is sample output of the **show platform hardware qfp active infrastructure statistics type punt-drop** command. The fields in the display are self-explanatory.

```
Router# show platform hardware qfp active infrastructure punt statistics type punt-drop

Punt Drop Statistics

  Number of punt causes = 97

  Drop Counter ID   0      Drop Counter Name PUNT_NOT_ENABLED_BY_DATA_PLANE

  Counter ID  Punt Cause Name                          Packets
  --------------------------------------------------------------------
  000         Reserved                                 0
  001         MPLS ICMP Can't Fragment                 0
  002         IPv4 Options                             0
  003         Layer2 control and legacy                0
```

```
  004         PPP Control                            0
…
```

show platform hardware qfp active interface if-name statistics

To display the statistics of packet drops for each interface in the Packet Processor Engine (PPE), use the **show platform hardware qfp active interface if-name statistics** command in privileged EXEC mode.

show platform hardware qfp active interface if-name *type number* **statistics**

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.0	This command was introduced.

Usage Guidelines

You can use this command for troubleshooting the problems on an interface in a PPE by analyzing the statistics of packet drops.

Examples

The following sample output from the **show platform hardware qfp active interface if-name statistics** command displays the statistics of packet drops on the Gigabit Ethernet interface 0/0/0.781 interface:

```
Router # show platform hardware qfp active GigabitEthernet0/0/0.781 if-name statistics

----------------------------------------------------------------
Receive Stats                                   Packets        Octets
----------------------------------------------------------------
  Ipv4                                              2           322
  Ipv6                                              0             0
  Tag                                               0             0
  McastIpv4                                         0             0
  McastIpv6                                         0             0
  Other                                             3           204

----------------------------------------------------------------
Transmit Stats                                  Packets        Octets
----------------------------------------------------------------
  Ipv4                                              2           178
  Ipv6                                              0             0
  Tag                                               0             0
  McastIpv4                                         0             0
  McastIpv6                                         0             0
  Other                                             0             0

----------------------------------------------------------------
Input Drop Stats                                Packets        Octets
---------------------------------------------------------------
Ipv4uRpfStrictFailed                                   5           590
Ipv6uRpfStrictFailed                                   5           590

----------------------------------------------------------------
Output Drop Stats                               Packets        Octets
```

```
-----------------------------------------------------------------
  The Egress drop stats were all zero

-----------------------------------------------------------------
Drop Stats Summary:
note: 1) these drop stats are only updated when PAL
         reads the interface stats.
      2) the interface stats include the subinterface

Interface                                       Rx Pkts             Tx Pkts
----------------------------------------------------------------------------
GigabitEthernet0/0/0.781                             25                   0
```

The following table describes the fields shown in the display.

Table 196: show platform hardware qfp active interface if-name statistics Field Descriptions

Field	Description
Receive Stats	Number of packets received.
Packets	Number of packets that are received.
Octets	Total number of bytes of the packets that are received.
Transmit Stats	Number of packets that are transmitted on an interface.
Input Drop Stats	The drop cause and the number of incoming packets that are dropped. • pv4uRpfStrictFailed - Specifies the number and bytes of packets that are dropped with this drop cause. • Ipv6uRpfStrictFailed - Specifies the number and bytes of packets that are dropped with this drop cause
Packets	Number of packets that are transmitted. • IPv4uRpfStrictFailed received 5 packets. • IPv6uRpfStrictFailed received 5 packets.
Octets	Total number of bytes of the packets that are received. • IPv4uRpfStrictFailed received 590 bytes of packets. • IPv6uRpfStrictFailed received 590 bytes of packets.
Output Drop Stats	Specifies the drop cause and the number of outgoing packets that are dropped.
Interface	Name of the interface.
Rx Pkts	Number of packets received on an interface.
Tx Pkts	Number of packets transmitted on an interface.

Related Commands

Command	Description
show platform hardware qfp active statistics drop	Displays the statistics of packet drops on all the interfaces in a PPE.

show platform hardware qfp statistics drop

To display the statistics of all the dropped packets on the Embedded Services Processor (ESP), use the **show platform hardwareqfp active statistics drop** command in privileged EXEC mode.

show platform hardware qfp {**active** | **standby**} **statistics drop**

Syntax Description

active	Active forwarding processor.
standby	Standby forwarding processor .

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.0	This command was introduced.
Cisco IOS XE Release 3.5	This command was modified for Cisco ASR 1000 Series Routers. A new drop type, PPPoECAC, was added to the**show platform hardware qfp active statistics drop** command.

Usage Guidelines

You can use this command for troubleshooting the problems on all the interfaces in a PPE by analyzing the statistics of packet drops.

You can use this command for troubleshooting the problems on all the interfaces in a packet processing engine (PPE) by analyzing the statistics of packet drops.

To improve the CPU utilization and memory of the Route Processor (RP) on Cisco ASR 1000 Series Router, the SRSM hardware feature has been implemented. When Call Admission Control (CAC) is enabled and the CAC threshold level is reached, the PPPoE packets are punted on the Embedded Service Processor (ESP) instead of being sent to the RP. Managing the PPPoE packets at the ESP level helps in controlling and minimizing RP CPU and memory utilization. A new drop type, PPPoECAC, is added to the**show platform hardware qfp active statistics drop** command which indicates the number of PPPoE Active Discovery Initiation (PADI) and PPPoE Active Discovery Request (PADR) packets rejected by the hardware due to call admission control.

Note The **show call admission statistics** command shows how many packets were dropped by the RP and the **show platform hardware qfp active statistics drop** command indicates how many packets were dropped by the ESP. A small number of packets are still dropped by the RP because it takes time for the drop message to reach the ESP. The actual number of packets dropped by SRSM is the total number of packets dropped by **show call admission statistics** and **show platform hardware qfp active statistics drop** commands.

Examples

The following sample output from the **show platform hardware qfp active statistics drop** command displays the statistics of packet drops on all the interfaces in a PPPoE:

```
Router# show platform hardware qfp active statistics drop

Global Drop Stats                         Packets              Octets
-------------------------------------------------------------------------
BadUidbSubIdx                               59187             4918277
Disabled                                     4725              373436
Ipv4NoAdj                                     219                9468
Ipv4uRpfStrictFailed                           10                1180
Ipv6uRpfStrictFailed                           10                1180
UnconfiguredIpv4Fia                          1589              132013
```

The following sample output of the **show platform hardware qfp active statistics drop** command shows the PPPoECAC packets dropped on the ESP when the CAC threshold level is reached:

```
Router# show platform hardware qfp active statistics drop

Global Drop Stats                         Packets              Octets
-------------------------------------------------------------------------
BadUidbIdx                                     80                7901
BadUidbSubIdx                               40374             2860531
Disabled                                     4765              375064
InjectErr                                      64                8350
Ipv4NoAdj                                       8                 776
Ipv4NoRoute                                 52608             5482626
Ipv6NoAdj                                       1                  79
MplsIpv6FragReq                                 1                1515
UnconfiguredIpv4Fia                          2412              215692
PPPoECAC                                     4648              171976
```

The following table describes the fields shown in the display.

Table 197: show platform hardware qfp active statistics drop Field Descriptions

Field	Description
Global Drop Stats	The reason for dropping packets. • pv4uRpfStrictFailed - Specifies the number and bytes of packets that are dropped with this drop cause. • Ipv6uRpfStrictFailed - Specifies the number and bytes of packets that are dropped with this drop cause
Packets	Number of packets that are dropped. • IPv4uRpfStrictFailed dropped 10 packets. • IPv6uRpfStrictFailed dropped 10 packets.
Octets	Total number of bytes of the packets that are dropped. • IPv4uRpfStrictFailed dropped 1180 bytes of packets. • IPv6uRpfStrictFailed dropped 1180 bytes of packets.

Related Commands

Command	Description
show platform hardware qfp interface	Displays information about an interface in the target flow processor.
show platform hardware qfp active interface if-name statistics	Displays the statistics of packet drops for each interface in the Packet Processor Engine (PPE).

show platform hardware qfp interface

To display information about an interface in the target flow processor, use the **show platform hardware qfp interface** command in privileged EXEC mode.

show platform hardware qfp {**active** | **standby**} **interface** {**all** [{**summary** | **statistics** [**drop_summary** [{**subinterface**}]] [{**clear_drop**}] [{**detail**}]}] | **dsp** {**client resource** *dsp-resource-id* | **global clear** | **stream** *stream-id*} | {**if-name** *name* | **if-handle** *handle*} [{**info** | **path** | **statistics** [**drop_summary** [{**subinterface**}]] | [{**clear_drop**}] | [{**detail**}]}] | **atm if-name** *name* **statistics** [{**clear_drop**}]}

Syntax Description

active	Specifies the active instance of the processor.
standby	Specifies the standby instance of the processor.
interface	Specifies interfaces.
all	Specifies all interfaces available on the processor.
summary	(Optional) Specifies the interface summary report.
statistics	(Optional) Specifies the statistics of transmitted and received packets.
drop_summary	(Optional) Specifies the drop status summary report.
subinterface	(Optional) Specifies the subinterface and the drop statistics.
clear_drop	(Optional) Clears the drop statistics after reading.
detail	(Optional) Shows drop cause IDs.
dsp	Specifies digital signal processor (DSP) statistics.
client	Specifies DSP client statistics.
resource	Specifies DSP client resource statistics.
dsp-resource-id	Combinet Packet Protocol (CPP) DSP resource ID.
global	Specifies DSP global statistics.
clear	Clears statistics after reading.
stream	Specifies DSP stream statistics.
stream-id	Stream ID.
if-name *name*	Specifies the name of an interface, interface type, and port number of the selected interface.
if-handle *handle*	Specifies the quantum flow processor (QFP) interface handle number.
info	(Optional) Specifies interface information.

path	(Optional) Specifies path information.
atm	Specifies information and statistics for the ATM interface.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. The **cpp** keyword was changed to **qfp**.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 3.8S	This command was modified. The **path** keyword was added.

Usage Guidelines

The **show platform hardware qfp interface** command displays information about the relationship between one interface and another in the target flow processor. In the command output, the main interface is identified if the interface is a subinterface; the group interface is identified if the interface is a member of a group; and the interfaces that are members of the group are identified if the interface is a group, bundle, or multipoint interface.

Examples

The following sample output shows information about the relationship between one interface and the other on the target flow processor:

```
Device# show platform hardware qfp active interface if-name Port-channel1 info

General interface information
  Interface Name: Port-channel1
  Platform interface handle: 36
  QFP interface handle: 36
  Rx uidb: 131064
  Tx uidb: 131036
  Channel: 0
Interface Relationships
  if_h   Member Interface Name
  10      GigabitEthernet0/0/2
  11      GigabitEthernet0/0/3
```

The table below describes the significant fields shown in the display.

Table 198: show platform hardware qfp interface Field Descriptions

Field	Description
Interface Name	Name of the interface requested by the **show platform hardware qfp interface** command.
Platform interface handle	Number of platform interface handles displayed for the interface.
QFP interface handle	Internal identifier assigned by the QFP software for this interface.
Rx uidb	Internal identifier for the receive side of the interface.

Field	Description
Tx uidb	Internal identifier for the transmit side of the interface.
Channel	Internal identifier for the transmit path to which the interface is connected.

The following sample output shows the summary of the drop status of the packets:

```
Device# show platform hardware qfp active statistics drop

Global Drop Stats                         Packets                  Octets
-------------------------------------------------------------------------
BadUidbIdx                                     80                    7901
BadUidbSubIdx                               40374                 2860531
Disabled                                     4765                  375064
InjectErr                                      64                    8350
Ipv4NoAdj                                       8                     776
Ipv4NoRoute                                 52608                 5482626
Ipv6NoAdj                                       1                      79
MplsIpv6FragReq                                 1                    1515
UnconfiguredIpv4Fia                          2412                  215692
```

The table below describes the significant fields shown in the display.

Table 199: show platform hardware qfp active statistics drop Field Descriptions

Field	Description
Global Drop Stats	Reason for dropping of packets.
Packets	Number of packets that are dropped.
Octets	Total number of bytes of the packets that are dropped.

The following sample output shows the statistics of the packets on an interface:

```
Device# show platform hardware qfp active interface if-name GigabitEthernet0/0/0.775
statistics

----------------------------------------------------------------
Receive Stats                             Packets         Octets
----------------------------------------------------------------
  Ipv4                                       9             810
  Ipv6                                       0               0
  Tag                                        0               0
  McastIpv4                                  0               0
  McastIpv6                                  0               0
  Other                                      2             136
----------------------------------------------------------------
Transmit Stats                            Packets         Octets
----------------------------------------------------------------
  Ipv4                                       0               0
  Ipv6                                       1             154
  Tag                                        0               0
  McastIpv4                                  0               0
  McastIpv6                                  0               0
  Other                                      0               0
----------------------------------------------------------------
Input Drop Stats                          Packets         Octets
```

```
---------------------------------------------------------------
Ipv4NoRoute                                   182        22996
MplsIpv6FragReq                                 1         1515
UnconfiguredIpv4Fia                           550        49120
----------------------------------------------------------------
Output Drop Stats                         Packets        Octets
---------------------------------------------------------------
Ipv4NoRoute                                    13         3721
----------------------------------------------------------------
Drop Stats Summary:
note: 1) these drop stats are only updated when PAL
         reads the interface stats.
      2) the interface stats include the subinterface
Interface                                      Rx Pkts             Tx Pkts
---------------------------------------------------------------------------
GigabitEthernet0/0/0.775                          3209                  20
```

The table below describes the significant fields shown in the display.

Table 200: show platform hardware qfp active interface if-name statistics Field Descriptions

Field	Description
Receive Stats	Number of packets received through a protocol.
Packets	Number of packets transmitted through a protocol.
Octets	Total number of bytes of the packets that are dropped.
Transmit Stats	Number of packets that are transmitted on an interface.
Input Drop Stats	Drop cause and the number of incoming packets that are dropped.
Output Drop Stats	Drop cause and the number of outgoing packets that are dropped.
Interface	Name of the interface.
Rx Pkts	Number of packets received on an interface.
Tx Pkts	Number of packets transmitted on an interface.

```
Device# show platform hardware qfp active interface if-handle 10 path

Hardware Path Information: Port type 2 - NGIO
Ingress Path Information:
Interface ID 1
IID table entry address 0x30b61018
Input uIDB 2043
Flow Control ID 0x30b61500
Egress Path Information:
Interface ID 1
FFP output port -2
Module backplane connection index 0
Switch port ID 8
Module number 0
MAC destination address c4: a:cb:56: 0:d5
MAC source address 30:f7: d:53:f4:db
```

The table below describes the significant fields shown in the display.

Table 201: show platform hardware qfp active interface if-handle path Field Descriptions

Field	Description
Hardware Path Information	Type of module on which the interface exists. Possible values are NGIO and BEST_EFFORT.
Ingress Path Information	Ingress path information.
Interface ID	Identifier assigned to the interface by the module. This identifier is local to the module.
IID table entry address	Address of the table of interfaces on the module in the forwarding plane memory.
Input uIDB	Input micro-interface descriptor block (uIDB) assigned to this interface.
Flow Control ID	Identifier for the flow control structure if the interface traffic is flow controlled.
Egress Path Information	Egress path information.
FFP output port	Port of the forwarding process that handles traffic on the interface.
Module backplane connection index	Identifier for the backplane connection of the module that handles the traffic on the interface.
Switch port ID	Identifier for the backplane switchport that handles the traffic for the interface.
Module number	Module identifier.
MAC destination address	MAC address in the headers of the packets that traverse the backplane switch.

```
Device# show platform hardware qfp active interface if-handle 14 path

Hardware Path Information:
Ingress Path Information:
Look-up class 1
Remap table entry:
  SPA Format 2
  Valid flag 1
  Marmot channel 0
  Indirect flag 1
  Input uIDB 1019
Egress Path Information:
Marmot header 0x2000000
SPA type 2
SPA header length 4
SPA header 0x0 0x0 0x0 0x0
  LP small header 0xd2 0xa9 0xe0 0x10
  HP header 0x0 0x0 0x1 0x0
  Cntl header 0xfa 0x28 0xd4 0x10
```

The table below describes the significant fields shown in the display.

Table 202: show platform hardware qfp active interface if-handle path Field Descriptions

Field	Description
Hardware Path Information	Type of module on which the interface exists.
Ingress Path Information	Ingress path information follows.
Look-up class	Look-up method used to identify the ingress interface.
Remap table entry	Entry of the remap table of the interface follows.
SPA format	Format of the Shared Port Adapter (SPA) header.
Valid Flag	Flag indicating whether entry in the remap table is valid. 1 is valid.
Marmot Channel	Channel in the Marmot chip through which traffic passes.
Indirect flag	Flag indicating whether the ingress interface is determined indirectly through the SPA header.
Input uIDB	Input micro-interface descriptor block (uIDB) assigned to the interface.
Egress Path Information	Egress path information follows.
Marmot header	Marmot header in the egress packets.
SPA type	Format of the SPA header.
SPA header length	Length of the egress SPA header, in bytes.
SPA header	Default SPA header of the egress packets.
LP small header	SPA header used for low priority (LP) packets.
HP header	SPA header used for high priority (HP) packets.
Cntl header	SPA header used for control packets.

Related Commands

Command	Description
show interfaces	Displays statistics for all interfaces configured on a device or on an access server.

show platform hardware slot

To display information about the processor in a chassis slot, use the **show platform hardware slot** command in privileged EXEC or diagnostic mode.

Cisco ASR 1000 Series SPA Interface Processors
show platform hardware slot *sip* {**dram statistics** | **eobc** {**interface** {**primary** | **standby**} {**rmon** | **status**} | **switch statistics** {**brief** | **detail**}} | **fan status** | **io-port** | **led status** | **mcu status** [**raw**] | **plim** {**buffer settings** [**detail**] | **cpu** | **qos input bandwidth** | **registers** *reg* | **statistics** [**internal**] | **status** [**internal**]} | **sensor** {**consumer** | **producer**} {*id* | **all**} | **serdes** {**registers** *reg* | **statistics** [**internal**] | **status** [**brief**]} | **spa** {**attributes** | **oir-statistics** | **status**}}

Cisco ASR 1000 Series Embedded Services Processors
show platform hardware slot *esp* {**dram statistics** | **eobc** {**interface** {**primary** | **standby**} {**rmon** | **status**} | **switch statistics** {**brief** | **detail**}} | **io-port** | **led status** | **sensor** {**consumer** | **producer**} {*id* | **all** } | **serdes** {**registers** *reg* | **statistics** [**internal**] | **status** [**brief**]}}

Cisco ASR 1000 Series Route Processors
show platform hardware slot *rp* {**alarms** {**audible** | **visual**} | **dram statistics** | **eobc** {**interface** {**primary** | **standby**} {**rmon** | **status**} | **switch statistics** {**brief** | **detail**}} | **io-port** | **led status** | **plim** {**buffer settings** [**detail**] | **cpu** | **qos input bandwidth** | **registers** *reg* | **statistics** [**internal**] | **status** [**internal**]} | **sensor** {**consumer** | **producer**} {*id* | **all**} | **serdes** {**registers** *reg* | **statistics** [**internal**] | **status** [**brief**]}}

Cisco ISR 4400 Series Routers
show platform hardware slot *sm* {**dram statistics** | **eobc** {**interface** {**primary** | **standby**} {**rmon** | **status**}} | **fan status** | **i95 stats** | **io-port** | **led status** | **mcu status** [**raw**] | **network-clocks** | **pcie** {**driver** {**layers** | **statistics** {**3pa** | **lsmpi** | **mux** | **octeon**}} | **status**} | **plim** {**buffer settings** [**detail**] | **cpu** | **qos input bandwidth** | **registers** *reg* | **statistics** [**internal**] | **status** [**internal**]} | **rommon status** | **sensor** {**consumer** | **producer**} {*id* | **all**} | **serdes** {**registers** *reg* | **statistics** [{**internal** | **clear**}] | **status** [{**brief** | **clear**}]} | **spa** {**attributes** | **oir-statistics** | **status**}}

Syntax Description

sip	Type of Cisco ASR 1000 Series SPA interface processor (SIP) with one of the following values: • **0**—SIP in chassis slot 0. • **1**—SIP in chassis slot 1. • **2**—SIP in chassis slot 2. • **P0**—Power supply slot 0. • **P1**—Power supply slot 1. • **P2**—Power supply slot 2. • **P3**—Power supply slot 3.
dram statistics	Displays error-correcting code (ECC) error statistics for DRAM (for Cisco Technical Support only).
eobc	Displays Ethernet out-of-band channel (EOBC) information.
interface primary	Displays primary EOBC interface information.

interface standby	Displays standby EOBC interface information.
rmon	Displays EOBC interface remote monitoring (RMON) information (for Cisco Technical Support only).
status	Displays EOBC interface status information (Physical Line Interface Module [PLIM] status and serializer/deserializer [SerDes] status are for Cisco Technical Support only).
switch statistics	Displays EOBC switch statistics.
brief	Displays summary information.
detail	Displays detailed information (for Cisco Technical Support only). This keyword is optional for PLIM buffer settings.
fan status	Displays fan software status.
io-port	Displays I/O port information.
led status	Displays LED states.
mcu status	Displays microcontroller unit (MCU) hardware status (for Cisco Technical Support only).
raw	(Optional) Displays MCU unparsed raw data (for Cisco Technical Support only).
plim	Displays PLIM information.
buffer settings	Displays PLIM buffer settings (for Cisco Technical Support only).
cpu	Displays CPU hyper threading (HT) bus information (for Cisco Technical Support only).
qos input bandwidth	Displays PLIM quality of service (QoS) input bandwidth information.
registers *reg*	It is the register name (for Cisco Technical Support only).
statistics	Displays statistics information.
internal	(Optional) Displays Cisco internal information (for Cisco Technical Support only).
sensor	Displays sensor information (for Cisco Technical Support only).
consumer	Displays sensor information from the consumer process (for Cisco Technical Support only).
producer	Displays sensor information from the producer process (for Cisco Technical Support only).
id	Displays the consumer or producer sensor ID number (for Cisco Technical Support only).
all	Displays a brief view of all sensors (for Cisco Technical Support only).
serdes	Displays serializer/deserializer (SerDes) information.

spa	Displays Cisco ASR 1000 Series SPA information.
attributes	Displays SPA attribute information (for Cisco Technical Support only).
oir-statistics	Displays SPA online insertion and removal (OIR) counters.
esp	Type of Cisco ASR 1000 Series Embedded Services Processor (ESP) with one of the following values: • **f0**—ESP in ESP slot 0. • **f1**—ESP in ESP slot 1.
rp	Type of Cisco ASR 1000 Series Route Processor (RP) with one of the following values: • **r0**—RP in RP slot 0. • **r1**—RP in RP slot 1.
alarms	Displays alarm states information (for Cisco Technical Support only). To display alarm status, use the **show facility-alarm status** command.
audible	Displays audible alarm states (for Cisco Technical Support only) information.
visual	Displays LED alarm states (for Cisco Technical Support only) information.
sm	Type of Cisco ISR 4400 Series Routers interface with one of the following values: • **0**—SM-Inter-Processor slot 0. • **F0**—Embedded Service Processor slot 0. • **P0**—Power supply slot 0. • **P1**—Power supply slot 1. • **P2**—Power supply slot 2. • **R0**—Route Processor slot 0.
i95 stats	Displays i95 driver statistics.
network-clocks	Displays network clock devices.
pcie status	Displays Peripheral Component Interconnect Express (PCIE) information.
pcie driver layers	Displays PCIE driver stacking information.
pcie driver statistics	Displays PCIE driver statistics.
rommon status	Displays ROM Monitor (ROMMON) status.

Command Modes

Privileged EXEC (#)

Diagnostic (diag)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.

Release	Modification
15.0(1)S	This command was modified. The minimum bandwidth and the priority mode that cannot be configured in Strict Priority mode are not displayed in the output. The HP policer BW field was added to the output.
Cisco IOS XE Release 3.8S	This command was modified. References to SIP (Cisco ASR 1000 Series Shared Port Adaptor Interface Processors) in command options were replaced with SM (Cisco Services-Ready Engine [SRE] service module) for Cisco ISR 4400 Series Routers only.

Examples

The following sample output from the **show platform hardware slot 0 eobc interface primary status** command displays EOBC interface status for a SIP in chassis slot 0. This command provides the status of the EOBC in the indicated slot.

```
Device# show platform hardware slot 0 eobc interface primary status

EOBC interface status
  EOBC : eth0, status : Active
    Line State : Up, Speed : 1Gbps, Link mode : Full
    Line Type : AUI, Autoneg : Disabled
    Addr : 10.0.3.0, Netmask : 255.255.0.0, HW Addr : 0000.0300.0000
    Rx pkts : 1292995, bytes : 316283357, dropped : 0 errors : 0
    Tx pkts : 1124534, bytes : 270172949, dropped : 0 errors : 0
```

The table below describes the significant fields shown in the display.

Table 203: show platform hardware slot 0 eobc interface primary status Field Descriptions

Field	Description
EOBC: eth0	Ethernet port.
status	Port status. “Active” or “Standby.”
Line State	Line status. “Up” or “Down.”
Speed	Bandwidth in gigabits per second (Gbps).
Link mode	Transmission mode. “Full” (full duplex) or “Half” (half duplex).
Line Type	Type of transceiver. “AUI” (attachment unit interface), “TP” (twisted pair), “MII” (media independent interface), “FIBER” (fiber optic), or “BNC” (Bayonette Neil-Concelman).
Autoneg	Autonegotiation. “Enabled” or “Disabled.”
Addr	IP address of the port.
Netmask	IP addressing netmask of the port.
HW Addr	MAC address of the port.
Rx pkts/bytes	Number of packets and bytes received.
Tx pkts/bytes	Number of packets and bytes transmitted.

Field	Description
Rx dropped	Number of received packets that were dropped.
Tx dropped	Number of transmitted packets that were dropped.
Rx errors	Number of packets received with errors.
Tx errors	Number of packets transmitted with errors.

The following sample output from the **show platform hardware slot 0 eobc switch statistics brief** command displays brief EOBC switch statistics for a SIP in chassis slot 0:

```
Device# show platform hardware slot 0 eobc switch statistics brief

Port: 4, Link state: Up, Mode: Full Duplex, Speed: 1000 Mbps
Ingress bytes  :            276915312    Egress bytes  :           349585709
Ingress packets:              1151944    Egress packets:             1320618
```

The table below describes the significant fields shown in the display.

Table 204: show platform hardware slot 0 eobc switch statistics brief Field Descriptions

Field	Description
Port	Port on the EOBC switch.
Link state	Link status. “Up” or “Down.”
Mode	Transmission mode. “Full Duplex” or “Half Duplex.”
Speed	Bandwidth in megabits per second (Mbps).
Ingress bytes	Number of bytes received on this port.
Egress bytes	Number of bytes transmitted through this port.
Ingress packets	Number of packets received on this port.
Egress packets	Number of packets transmitted through this port.

The following sample output from the **show platform hardware slot 0 fan status** command displays fan operation status for a SIP in chassis slot 0:

```
Device# show platform hardware slot 0 fan status

Fan speed: 65%
Fan 0: Normal
Fan 1: Normal
Fan 2: Normal
```

The table below describes the significant fields shown in the display.

Table 205: show platform hardware slot 0 fan status Field Descriptions

Field	Description
Fan speed	Speed at which the fans are spinning as a percentage of their maximum speed.
Fan 0, 1, 2	Specifies whether a fan is encountering a fault condition. “Normal” or “Fail.”

The following sample output from the **show platform hardware slot 0 plim qos input bandwidth** command displays the ingress arbiter settings for all PLIM buffers that are in use for a SIP in chassis slot 0:

```
Device# show platform hardware slot 0 plim qos input bandwidth

Ingress QOS Scheduling Mode: Strict Priority

0/0, SPA-3XOC3-ATM-V2
  Interface 0/0/0
    BW:   155520 Kbps, Min BW: N/A , Excessive Weight:   100000 Kbps, HP Policer BW:
155520 Kbps
  Interface 0/0/1
    BW:   155520 Kbps, Min BW: N/A , Excessive Weight:   155000 Kbps, HP Policer BW:
155520 Kbps
  Interface 0/0/2
    BW:   155520 Kbps, Min BW: N/A , Excessive Weight:   155000 Kbps, HP Policer BW:
155520 Kbps
```

The table below describes the significant fields shown in the display.

Table 206: show platform hardware slot 0 plim qos input bandwidth Field Descriptions

Field	Description
Ingress QOS Scheduling Mode	Current scheduler operation mode.
BW	Interface bandwidth in kilobits per second (kb/s).
Min BW	Guaranteed bandwidth assigned on this interface in Kbps.
Excessive Weight	Excessive bandwidth assigned on this interface in Kbps.
HP Policer BW	Bandwidth assigned for processing high-priority traffic on this interface in Kbps.

The following sample output from the **show platform hardware slot 0 plim statistics** command displays PLIM statistics for a SIP in chassis slot 0. Interprocess communication (IPC) packets are internal control packets. The first set of RX and TX packet counts include both user packets and IPC packets. In this example, the RX/TX and RX IPC/TX IPC packet counts are the same because only IPC packets are being passed (no user packets).

```
Device# show platform hardware slot 0 plim statistics

1/0, 2XOC3-POS, Online
  RX Pkts 739     Bytes 54564
  TX Pkts 739     Bytes 30752
  RX IPC Pkts 739     Bytes 54564
  TX IPC Pkts 739     Bytes 30752
```

The table below describes the significant fields shown in the display.

Table 207: show platform hardware slot 0 plim statistics Field Descriptions

Field	Description
RX Pkts	Packets (user data and IPC data) received by the PLIM from the indicated SPA.
TX Pkts	Packets (user data and IPC data) transmitted from the PLIM to the indicated SPA.
RX IPC Pkts	IPC packets received by the PLIM from the indicated SPA.
TX IPC Pkts	IPC packets transmitted from the PLIM to the indicated SPA.

The following is sample output from the **show platform hardware slot f0 serdes statistics** command for Cisco ASR1000-ESP20 and later versions of the ESP. This output displays the byte counters and packet counters associated with the Enhanced SerDes Interconnect (ESI) links for the ESP. The output includes information about drop counters and the number of link-level flow control messages. Information is displayed from the standpoint of the card (in this example, ESP0), where the command is run. An ESP displays information from all the cards with active ESI links connected to it. A SIP or an RP displays statistics from each ESP.

```
Device# show platform hardware slot f0 serdes statistics

From Slot R0
  Pkts High: 0 Low: 0 Bad: 0 Dropped: 0
  Bytes High: 0 Low: 0 Bad: 0 Dropped: 0
  Pkts Looped: 0 Error: 0
  Bytes Looped 0
  Qstat count: 0 Flow ctrl count: 25671
To Slot R0
  Pkts High: 0 Low: 0
From Slot 0
  Pkts High: 0 Low: 0 Bad: 0 Dropped: 0
  Bytes High: 0 Low: 0 Bad: 0 Dropped: 0
  Pkts Looped: 0 Error: 0
  Bytes Looped 0
  Qstat count: 0 Flow ctrl count: 25674
To Slot 0
  Pkts High: 0 Low: 0
```

The table below describes the significant fields shown in the display.

Table 208: show platform hardware slot f0 serdes statistics Field Descriptions

Field	Description
From Slot	Information on data passed from the indicated processor to the card where the command is run and over the SerDes.
To Slot	Information on data passed to the indicated processor from the card where the command is run and over the SerDes.
Pkts/Bytes High	Number of packets and bytes of high priority data payload.
Pkts/Bytes Low	Number of packets and bytes of low priority data payload.

Field	Description
Pkts/Bytes Bad	Number of packets received with packet length errors or cyclic redundacy check (CRC) errors.
Pkts/Bytes Dropped	Number of bit bucket packets or bytes dropped.
Pkts/Bytes Looped	Number of packets looped back in loopback mode.
Pkts Error	Number of packets with errors.
Qstat count	Number of queue status messages received.
Flow ctrl count	Number of link-level flow control messages.

The following is sample output from the **show platform hardware slot f0 serdes statistics** command for the Cisco ASR1000-ESP10.

```
Device# show platform hardware slot f0 serdes statistics

From Slot R0
  Pkts High: 0 Low: 0 Bad: 0 Dropped: 0
  Bytes High: 0 Low: 0 Bad: 0 Dropped: 0
  Pkts Looped: 0 Error: 0
  Bytes Looped 0
  Qstat count: 0 Flow ctrl count: 25671
From Slot 0
  Pkts High: 0 Low: 0 Bad: 0 Dropped: 0
  Bytes High: 0 Low: 0 Bad: 0 Dropped: 0
  Pkts Looped: 0 Error: 0
  Bytes Looped 0
  Qstat count: 0 Flow ctrl count: 25674
```

The following is sample output from the **show platform hardware slot f0 serdes statistics internal** command for the Cisco ASR 1000-ESP10.

```
Device# show platform hardware slot f0 serdes statistics internal

Load for five secs: 35%/8%; one minute: 33%; five minutes: 30%
Time source is NTP, 12:20:00.746 IST Fri Nov 9 2011
Network-Processor Link:
  Local TX in sync, Local RX in sync
  From Network-Processor    Packets:     1150522  Bytes:   166031138
  To Network-Processor      Packets:     4364008  Bytes:   697982854

RP/ESP Link:
Local TX in sync, Local RX in syncxist
Remote TX in sync, Remote RX in sync
To RP/ESP                 Packets:     1150522  Bytes:   166031138
 Drops                   Packets:           0  Bytes:           0
From RP/ESP               Packets:     4364008  Bytes:   697982854
 Drops                   Packets:           0  Bytes:           0
Errors:
 RX/TX process: 0/0, RX/TX schedule: 0/0
 RX/TX statistics: 0/0, RX parity: 0

Encryption Processor Link:
  Local TX in sync, Local RX in sync
  Remote TX in sync, Remote RX in sync
```

The following is sample output from the **show platform hardware slot f0 serdes statistics internal** command for the Cisco ASR 1000-ESP20 and later versions of the ESP.

```
Device# show platform hardware slot f0 serdes statistics internal

Load for five secs: 35%/8%; one minute: 33%; five minutes: 30%
Time source is NTP, 12:20:00.746 IST Fri Nov 9 2011
Network-Processor Link:
  Local TX in sync, Local RX in sync
  From Network-Processor    Packets:     1150522  Bytes:   166031138
  To Network-Processor      Packets:     4364008  Bytes:   697982854

Encryption Processor Link:
  Local TX in sync, Local RX in sync
  Remote TX in sync, Remote RX in sync
```

The following sample output from the **show platform hardware slot 0 spa oir-statistics** command displays the OIR statistics of SPAs installed in a SIP in chassis slot 0:

```
Device# show platform hardware slot 0 spa oir-statistics

 SPA OIR requests: : 3
SPA OIR responses: : 3
   SPA insertions: : 0
     SPA removals: : 0
SPA driver starts: : 0
 SPA driver stops: : 0
SPA driver deaths: : 0
```

The table below describes the significant fields shown in the display.

Table 209: show platform hardware slot 0 spa oir-statistics Field Descriptions

Field	Description
SPA OIR requests	Number of times the chassis software on the SIP made a request to the chassis software on the RP to allow a SPA to come online.
SPA OIR responses	Number of times the chassis software on the RP sent a response to an OIR request to the chassis software on the SIP.
SPA insertions	Number of SPA insertions since the last boot. The number is zero for SPAs that were in the chassis when the chassis booted.
SPA removals	Number of SPA removals since the last boot.
SPA driver starts	Number of times the SPA driver started.
SPA driver stops	Number of times the SPA driver stopped.
SPA driver deaths	Number of time the SPA driver reloaded.

The following sample output from the **show platform hardware slot P0 mcu status** displays the MCU hardware status and power supply in the slot:

If you use the **show platform hardware slot** *sip* **mcu status** command or the **show platform hardware slot** *sip* **fan status** command on the Cisco ASR 1000 Series Router, we recommend that you use the value “Px” rather than “0” or other numeric values to specify the power supply slot. This command displays the MCU hardware status or fan status and references the power supply in the slot.

```
Device# show platform hardware slot P0 mcu status

Model ID: 5
12V I: 31
12V V: 11
Temp: 29
Input V: 218
Fan speed: 65%
```

The table below describes the significant fields shown in the display.

Table 210: show platform hardware slot mcu status Field Descriptions

Field	Description
Model ID	Model ID of the card slot.
12V	Power supply in the slot in voltage.
Temp	Chassis temperature.
Input V	Voltage input for power supply.
Fan speed	Speed at which the fans are spinning as a percentage of their maximum speed.

Related Commands

Command	Description
show platform hardware interface	Displays information about an interface.
show platform hardware port	Displays information about an interface port on an SPA.
show platform hardware subslot	Displays information about an SPA.

show platform hardware throughput crypto

To display throughput information on a physical router, use the **show platform hardware throughput crypto** command in privileged EXEC mode. The output displays the configured throughput level, indicates if hardware throttling is effective and what the system-imposed limit is, the default throughput level for the device, and the configured boot level license.

show platform hardware throughput crypto

Command Default

Privileged EXEC (#)

Command Modes

No default behavior or values.

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.2	This command was introduced on Cisco Catalyst 8300, and 8500 Series Edge Platforms.
Cisco IOS XE Bengaluru 17.4.1	This command was introduced on the Cisco Catalyst 8200 Series Edge Platforms
Cisco IOS XE Cupertino 17.9.3a	The text in the output was modified to make it easier to understand.

Usage Guidelines

The output of the command provides the following information related to the throughput level on a physical router:

- It displays the throughput level that is currently effective. This value is configured with the **platform hardware throughput crypto** command in global configuration mode. If a level is not configured, the default is effective.

  The value here can be a numeric value or a tier-based throughput value. Support for tier-based throughput values was introduced in Cisco IOS XE Cupertino 17.7.1a. For more information, see Tier and Numeric Throughput Mapping for Physical Platforms, Cisco IOS XE Cupertino 17.8.1a and Later Releases.

- It indicates if the value is saved in the startup configuration file. If a configured value is not saved, it does not persist across reloads.

- It displays the hardware throttling limit that the configured value falls under. This is system-determined. See device-specific details in the following table: Throughput and System Hardware Throttling Specifications in the Autonomous Mode.

- It specifies the throttling limit that is finally effective. This value will account for aggregate throughput throttling if it is effective. Support for aggregate throughput throttling was introduced in Cisco IOS XE Cupertino 17.8.1a.

- It displays the default throughput level of the device.

- It displays the boot-level DNA license that is configured on the device.

The following is sample output of the **show platform hardware throughput crypto** command on a Cisco Catalyst 8300 Series Edge Platform (C8300-2N2S-4T2X). The software version running on the device is earlier than Cisco IOS XE Cupertino 17.9.3a:

```
Device# show platform hardware throughput crypto
Current configured crypto throughput level: 250M
     Level is saved, reboot is not required
Current enforced crypto throughput level: 250M
Crypto Throughput is throttled at 250M
Default Crypto throughput level: 10M
Current boot level is network-advantage
```

The following is sample output of the **show platform hardware throughput crypto** command on a Cisco Catalyst 8300 Series Edge Platform (C8300-2N2S-4T2X). The software version running on the device is Cisco IOS XE Cupertino 17.9.3a. From the output you can derive these key conclusions:

- The throughput level that is effective is 10 Mbps.
- Configuration is saved in the startup configuration file; the configured value will therefore persist across reloads.
- From table Throughput and System Hardware Throttling Specifications in the Autonomous Mode, we know that on a C8300-2N2S-4T2X, for any throughput level up to 250 Mbps, the hardware-imposed throttling limit is 250 Mbps.
- Throughput is throttled at 250 Mpbs. Note that aggregate throughput throttling is not applicable when the configured throughput is lesser than or equal to 250 Mbps.

```
Device# show platform hardware throughput crypto
Current configured crypto throughput level: 10M
     Level is saved, reboot is not required
Configured crypto throughput level on rate limiter: 250M
Crypto Throughput will be rate limited at 250M
Default Crypto throughput level: 10M
Current boot level is network-essentials
```

The following is sample output of the **show platform hardware throughput crypto** command on a Cisco Catalyst 8300 Series Edge Platform (**C8300-1N1S-4T2X**). The software version running on the device is Cisco IOS XE Cupertino 17.9.3a. From the output you can derive these key conclusions:

- The throughput level that is effective is T3.
- On C8300-1N1S-4T2X, T3 is the equivalent of 2.5 Gbps.
- Configuration is saved in the startup configuration file; the configured value will therefore persist across reloads.
- On a C8300-1N1S-4T2X, when a throughput level of T3 (2.5 Gbps) is configured, the system lifts all throttling restrictions.

```
Device# show platform hardware throughput crypto
Current configured crypto throughput level: T3
     Level is saved, reboot is not required
Configured crypto throughput level on rate limiter: 2.5G
Crypto Throughput will not be rate limited
Default Crypto throughput level: 10M
Current boot level is network-premier
```

Related Commands

Command	Description
platform hardware throughput crypto	Configures a throughput value on a physical router.

show platform hardware throughput level

To display the current maximum throughput level for a virtual router, use the **show platform hardware throughput level** command in Privileged EXEC mode.

show platform hardware throughput level

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.9S	This command was introduced on the Cisco CSR 1000V Cloud Services Router.

Usage Guidelines

The maximum throughput level is determined by the installed license. Depending on the configuration and installed license, you can change the maximum throughput level. See the **platform hardware throughput level** command for more information.

Example

The following example displays the maximum throughput level on the router:

```
Router# show platform hardware throughput level
The current throughput level is 50000 kb/s
```

Related Commands

Command	Description
platform hardware throughput level	Changes the maximum throughput level on the virtual router.

show platform hardware subslot

To display information about a Cisco ASR 1000 Series shared port adapter (SPA), use the **showplatformhardwaresubslot**command in privileged EXEC or diagnostic mode.

show platform hardware subslot *slot/card* **plim** {**buffer** [**settings detail**] | **qos input bandwidth** | **spa settings** | **statistics** [**internal**]}

Syntax Description

slot /	Chassis slot where the Cisco ASR 1000 Series SPA interface processor (SIP) is installed.
card	Secondary slot number of the SIP where the SPA is installed.
plim	Provides Physical Line Interface Module (PLIM) information.
buffer	Provides PLIM buffer information (for Cisco Technical Support only).
settings detail	(Optional) Provides detailed PLIM buffer settings (for Cisco Technical Support only).
qos input bandwidth	Provides PLIM QoS input bandwidth information.
spa settings	Provides PLIM SPA settings (for Cisco Technical Support only).
statistics	Provides PLIM statistics.
internal	(Optional) Provides PLIM detailed statistics information (for Cisco Technical Support only).

Command Modes

Privileged EXEC (#) Diagnostic (diag)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Routers.
15.0(1)S	This command was modified. The minimum bandwidth and the proirity mode that cannot be configured in Strict Priority mode are not displayed in the output. The HP policer BW field was added to the output.

Examples

The following example displays ingress arbiter settings for all PLIM buffers that are in use for a SPA in chassis slot 1:

```
Router# show platform hardware subslot 1/0 plim qos input bandwidth
Ingress QOS Scheduling Mode: Strict Priority

0/0, SPA-3XOC3-ATM-V2
  Interface 0/0/0
    BW:   155520 Kbps, Min BW: N/A , Excessive Weight:   100000 Kbps, HP Policer BW:
155520 Kbps
  Interface 0/0/1
    BW:   155520 Kbps, Min BW: N/A , Excessive Weight:   155000 Kbps, HP Policer BW:
```

```
155520 Kbps
  Interface 0/0/2
    BW:   155520 Kbps, Min BW: N/A , Excessive Weight:   155000 Kbps, HP Policer BW:
155520 Kbps
```

The table below describes the significant fields shown in the display.

Table 211: show platform hardware subslot 1/0 plim qos input bandwidth Field Descriptions

Field	Description
Ingress QOS Scheduling Mode	Current scheduler operation mode.
BW	Interface bandwidth in kilobits per second (kb/s).
Min Bw	Guaranteed bandwidth assigned on this interface in kb/s.
Excessive Weight	Excessive bandwidth assigned on this interface in kb/s.
HP Policer BW	Bandwidth assigned for processing high priority traffic on this interface in kb/s.

The following example displays PLIM statistics for a SPA in chassis slot 1. Interprocess communication (IPC) packets are internal control packets. The first set of RX and TX packet counts includes both user packets and IPC packets. In this example, the RX/TX and RX IPC/TX IPC packet counts are the same because no user packets are being passed, only IPC packets.

```
Router# show platform hardware subslot 1/0 plim statistics
1/0, 2XOC3-POS, Online
  RX Pkts 739     Bytes 54564
  TX Pkts 739     Bytes 30752
  RX IPC Pkts 739     Bytes 54564
  TX IPC Pkts 739     Bytes 30752
```

The table below describes the significant fields shown in the display.

Table 212: show platform hardware subslot 1/0 plim statistics Field Descriptions

Field	Description
RX Pkts	Packets (user data and IPC data) received by the PLIM from the indicated SPA.
TX Pkts	Packets (user data and IPC data) transmitted from the PLIM to the indicated SPA.
RX IPC Pkts	IPC packets received by the PLIM from the indicated SPA.
TX IPC Pkts	IPC packets transmitted from the PLIM to the indicated SPA.

Related Commands

Command	Description
show platform hardware interface	Displays information about an interface.
show platform hardware port	Displays information about an interface port on a shared port adapter (SPA).
show platform hardware slot	Displays information about the processor in a chassis slot.

show platform hardware subslot (4400)

To display information on the network interface module, use the **show platform hardware subslot** command in privileged EXEC mode.

show platform hardware subslot *slot/bay* **module** [{ **firmware** | **status** | **device** *device-name* | **host-if** | [{**statistics** | **status** | **register**}]}]

Syntax Description

slot/ bay	Specifies the chassis slot and secondary slot number where the module is installed.
module	Specifies the module information.
firmware	Displays the firmware and bootloader version.
status	Displays information on the firmware operational status, CPU, and memory utilization.
device	Displays information for specific module devices.
device-name	Specifies the device.
host-if	Specifies the host interface.
statistics	(Optional) Displays the link statistics for the host interface.
status	(Optional) Displays the configuration, status, and interface ID for the host interface.
register	(Optional) Displays the register information for the host interface.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced.

Example

The following are sample outputs from the **show platform hardware subslot module** command.

```
Router# show platform hardware subslot 0/1 module host-if status

NPU global_info:
CP_MAC:     0x30.f7.0d.53.bc.9e
FFP_MAC:    0x30.f7.0d.53.bc.9b
Module_MAC: 0x0c.d9.96.a8.01.cc
DSP_MAC:    0x00.00.00.00.00.00
CP VLAN ID:    0x09 0x2f
FFP VLAN ID:    0x29 0x2e
FFP HP1 VLAN ID: 0x89 0x2e
FFP HP2 VLAN ID: 0xa9 0x2e
Max MTU 10442
```

```
Router# show platform hardware subslot 0/1 module host-if statistics

GE (connecting to BP switch) statistics

                Rx frames       Rx Bytes        Tx frames       Tx Bytes
------------------------------------------------------------------------------
pkt forwarded   744             51328           691             101687
oversize        0                               2
undersize       0                               0
multicast       0                               0
broadcast       0                               2
pause           0                               0
dropped         0                               0
FCS err         0                               0
aligmt err      0
length err      0
MRU err         0
SDU err         0
overrun err     0
undrrun err                                     0


Total frames
------------------------------------------------------------------------------
64              696
65 ~ 127        195
128 ~ 255       529
256 ~ 511       11
512 ~ 1023      2
1024 ~ 1518     0
1519 ~ 1522     0

Flow Aggregation to BP switch
------------------------------------------------------------------------------
FlowControl FA
        pkt fowarded:18 bytes forwarded:576
        fpb drop:0 mtu drop:0 tx_q drop:0
DSP signaling FA
        pkt fowarded:0 bytes forwarded:0
        fpb drop:0 mtu drop:0 tx_q drop:0
DSP media FA
        pkt fowarded:0 bytes forwarded:0
        fpb drop:0 mtu drop:0 tx_q drop:0
Low priorty FA (IP/ARP/BC)
        pkt fowarded:2 bytes forwarded:1180
        fpb drop:0 mtu drop:0 tx_q drop:0
Control message FA
        pkt fowarded:670 bytes forwarded:96285
        fpb drop:0 mtu drop:0 tx_q drop:0

Router# show platform hardware subslot 0/1 module firmware


Chip Revision: unknown

WDDI Build: 1771
WinFarm-0:DPS Build: 2220
WinFarm-1:DPS Build: 2220

WF-0 features set:
70d43f57 7987fffe 30f80386 46809a62 016d100e
c780344e 38357dd1 01940200 00000000 00000000
00000000 00000000 00000000 00000000 50c55135
```

```
WF-1 features set:
70d43f57 7987fffe 30f80386 46809a62 016d100e
c780344e 38357dd1 01940200 00000000 00000000
00000000 00000000 00000000 00000000 50c55135


Linux version 2.6.28.10.mips-malta (sheaunt@mcp-bld-lnx-101) (gcc version 4.3.3 (MontaVista
 Linux Sourcery G++ 4.3-302) ) #2 PREEMPT Wed Feb 27 19:14:01 PST 2013


Bootloader version: 0.1
FPGA (Active) version: 12120415
FPGA (Upgraded) version: 12120415

Router# show platform hardware subslot 0/1 module status


Process and Memory
---------------------------------
Mem: 39640K used, 12464K free, 0K shrd, 0K buff, 27492K cached
CPU:   0% usr   0% sys   0% nic 100% idle   0% io   0% irq   0% sirq
Load average: 0.00 0.00 0.00 1/17 198
  PID  PPID USER     STAT   VSZ %MEM %CPU COMMAND
  156   155 0        S     122m 240%   0% [cisco_fortitude]
    1     0 0        S     3452   7%   0% sh
  197   196 0        S     3080   6%   0% /bin/sh ./fortitude_moduleinfo.sh Proc
  196   156 0        S     3016   6%   0% sh -c ./fortitude_moduleinfo.sh "Proce
  198   197 0        R     3016   6%   0% /usr/bin/top -b -n 1 -d 30
  155   154 0        S     1852   4%   0% ./Supervisory
  154     1 0        S     1788   3%   0% ./Supervisory
    2     0 0        SW<      0   0%   0% [kthreadd]
    3     2 0        SW<      0   0%   0% [ksoftirqd/0]
    4     2 0        SW<      0   0%   0% [events/0]
    5     2 0        SW<      0   0%   0% [khelper]
    6     2 0        SW<      0   0%   0% [kblockd/0]
    7     2 0        SW       0   0%   0% [pdflush]
    8     2 0        SW       0   0%   0% [pdflush]
    9     2 0        SW<      0   0%   0% [kswapd0]
   10     2 0        SW<      0   0%   0% [aio/0]
   19     2 0        SW<      0   0%   0% [mtdblockd]




Interrupts
---------------------------------
           CPU0
  2:          0           MIPS  WinPath interrupt controller
  7:   26845968           MIPS  timer
  8:          0     WinPath-PIC  sys_err_handler
  9:          0     WinPath
```

show platform hardware transceiver

To see transceiver information on a port, use the show platform hardware transceiver command in EXEC mode.

show platform hardware transceiver {**brief** | **status** | **config** | **error** | **register**} [**port**]

Syntax Description

brief	Brief device information.
status	Device status.
config	Device configuration.
error	Device error information.
register	Device register contents.
port	Specifies the port. If you do not select a port, this command will iterate through all ports.

Command Default

No default behavior or values

Command Modes

EXEC (#)

Command History

Release	Modification
12.2(33)SRD	This command was introduced on the Cisco 7600 series routers. **Note** This command applies only to the Cisco 7600 Series Ethernet Services Plus (ES+) line card on the Cisco 7600 series router.

Usage Guidelines

Use this command with the remote command command in EXEC mode.

Examples

The following example shows brief information for port 1.

```
Router# remote command module 13 show platform hardware transceiver brief 1
Show brief info for port 1:
GigabitEthernet13/1:
        ID: SFP
        Extended ID: 4
        Xcvr Type: GE SX (13)
        Connector: LC
        Vendor name: CISCO-FINISAR
        Vendor part number: FTLF8519P2BCL-CS
        State: Enabled
```

The following example shows status information for port 1.

```
Router# remote command module 13 show platform hardware transceiver status 1
Show status info for port 1:
TenGigabitEthernet1/1:
        State: Enabled
        Environmental Information - raw values
```

```
            Temperature: 7616
            Tx voltage: 0 in units of 100uVolt
            Tx bias: 28722 uA
            Tx power: -2 dBm (5441 in units of 0.1 uW)
            Rx power: 0 dBm (7712 in units of 0.1 uW)
            (AUX1) Laser Temperature: 8704
            (AUX2) +3.3V Supply Voltage: 32928
    XFP TX is enabled.
    XFP TX is soft enabled.
    XFP is ready.
    XFP is not power down.
    XFP is not soft power down.
    XFP doesn't have interrupt(s).
    XFP is not LOS.
    XFP data is ready.
    XFP TX path is ready.
    XFP TX laser is not in fault condition.
    XFP TX path CDR is locked.
    XFP RX path is ready.
    XFP RX path CDR is locked.
    No active alarms
    No active warning
```

Related Commands

Command	Description
remote command {module num | standby-rp | switch} command	Executes a Cisco 7600 series router command directly on the switch console or a specified module without having to log into the Cisco 7600 series router first.

show platform isg memory

To display dynamically allocated memory usage information on the route processor (RP), use the **showplatformisgmemory**command in privileged EXEC mode.

show platform isg memory [**detail**]

Syntax Description

detail	(Optional) Displays detailed memory usage information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)S	This command was introduced.

Examples

This is a sample output of the **showplatformisgmemory**command.

```
Router# show platform isg memory
Allocator-Name                  In-use/Allocated           Count
  ----------------------------------------------------------------------------
  CWAN VRF NODE            :          0/65588      (  0%) [       0] Chunk
  CWAN PLATFORM            :          0/20052      (  0%) [       0] Chunk
  CWAN PPPoE SB            :          0/20052      (  0%) [       0] Chunk
  CWAN PPPOE NOD           :          0/65588      (  0%) [       0] Chunk
  CWAN VRF Sess Cnt        :      16384/16436      ( 99%) [       1]
  CWAN MSI Array           :      16384/16436      ( 99%) [       1]
  CWAN MSI Elem            :      98304/311296     ( 31%) [    4096]
  VRF Pend list Array      :      16384/16436      ( 99%) [       1]
  VRF Pend list MSI        :      98304/311296     ( 31%) [    4096]
  CWAN slot pid hdl        :         60/112        ( 53%) [       1]
  CWAN sess per slot       :    2880000/2880780    ( 99%) [      15]
  CWAN test lru hdl        :         24/76         ( 31%) [       1]
  CWAN Container HWSB      :         56/108        ( 51%) [       1]
  CW Cont swidb SB         :        104/208        ( 50%) [       2]
  L4R Rules per            :          0/32820      (  0%) [       0] Chunk
  L4R Srv Grps p           :          0/32820      (  0%) [       0] Chunk
  L4R non-access           :          0/65588      (  0%) [       0] Chunk
  L4R Srv Info             :          0/32820      (  0%) [       0] Chunk
```

The table below describes the fields shown in the **showplatformisgmemory**command display.

Table 213: show platform isg memory Field Descriptions

Field	Description
Allocator-Name	Name of the memory allocating process.
In-use	Indicates the current memory usage.
Allocated	Total memory allocated by the process.
Count	Number of allocated memory blocks.

show platform mgf

To show the details of the multi-gigabit fabric, use the **show platform mgf** command in privileged EXEC mode.

show platform mgf [{**module** | **statistics cpu**}]

Syntax Description

module	Shows details of the modules registered to the backplane switch manager (BPSM).
statistics	Displays the multi-gigabit fabric's packet statistics.
cpu	Displays the multi-gigabit fabric's cpu port statistics.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced for the Cisco 3900 Series, 2900 Series, and 1900 Series Integrated Services Routers (ISRs).

Usage Guidelines

To show the details of the multi-gigabit fabric, use the **show platform mgf** command in privileged EXEC mode. Or, enter the **show platform mgf** command and press Enter to display VLAN and slot assignments on the router. An asterisk next to the slot indicates that the vlan is the slot's default VLAN. The following example displays output from a Cisco 3945 ISR.

Note Before Cisco IOS 15.1(3)T release, the Cisco Services Ready Engine (SRE) Service Module was managed by the platform backplane code. Therefore, when you entered the **show platform mgf** command, the Cisco SRE Service Module was displayed in the command output. But with Cisco IOS 15.1(3)T release, because the Cisco SRE Service Module is in the switchport managed module, it is no longer displayed in the **show platform mgf** command output.

Note VLAN1 is the default when no other VLAN are listed.

```
Router# show platform mgf
VLAN    Slots
------------------------------------------------------------
1       ISM*, EHWIC-0*, EHWIC-1*, EHWIC-2*, EHWIC-3*
        PVDM-0*, PVDM-1*, PVDM-2*, PVDM-3*, SM-1*
        SM-2*, SM-3*, SM-4*
```

Examples

The following example displays the output for the **show platform mgf module** command when entered on a Cisco 3945 ISR. The table below displays the information code that appears in the output.

```
Router# show platform mgf module
Registered Module Information
Code:   NR - Not Registered, TM - Trust Mode, SP - Scheduling Profile
        BL - Buffer Level, TR - Traffic Rate, PT - Pause Threshold
slot    vlan    type/ID         TM      SP      BL      TR      PT
----    ----    ----------      ------- ---     ------  -----   ----
ISM     NR
EHWIC-0 NR
EHWIC-1 NR
EHWIC-2 NR
EHWIC-3 NR
PVDM-0  NR
PVDM-1  NR
PVDM-2  NR
PVDM-3  NR
SM-1     1       SM/6            UP      1       high    1000    high
SM-2     1       SM/6            UP      1       high    1000    high
SM-3    NR
SM-4    NR
```

Table 214: Show Platform Backplane Module Information Code

Code	Description
NR	Not registered
TM	Trust mode
SP	Scheduling profile
BL	Buffer level
TR	Traffic rate
PT	Pause threshold

The following example displays output for the **show platform mgf statistics** command when entered on a Cisco 1941 ISR.

```
Router# show platform mgf statistics

Interface statistics for slot: ISM (port 1)
-----------------------------------------------------
30 second input rate 0 packets/sec
30 second output rate 0 packets/sec
0 packets input, 0 bytes, 0 overruns
Received 0 broadcasts, 0 multicast, 0 unicast 0 runts, 0 giants, 0 jabbers 0 input errors,
 0 CRC, 0 fragments, 0 pause input 0 packets output, 0 bytes, 0 underruns 0 broadcast, 0
multicast, 0 unicast 0 late collisions, 0 collisions, 0 deferred 0 bad bytes received, 0
multiple, 0 pause output
Interface statistics for slot: EHWIC-0 (port 2)
-----------------------------------------------------
30 second input rate 13844 packets/sec
30 second output rate 13844 packets/sec
3955600345 packets input, 1596845471340 bytes, 26682 overruns Received 0 broadcasts, 0
```

```
multicast, 3955600345 unicast 0 runts, 0 giants, 0 jabbers 0 input errors, 0 CRC, 0 fragments,
 0 pause input
3955738564 packets output, 1596886171288 bytes, 0 underruns 0 broadcast, 0 multicast,
3955738564 unicast 0 late collisions, 0 collisions, 0 deferred 0 bad bytes received, 0
multiple, 94883 pause output
Interface statistics for slot: EHWIC-1 (port 3)
-----------------------------------------------------
30 second input rate 13844 packets/sec
30 second output rate 13844 packets/sec
3955973016 packets input, 1598763291608 bytes, 26684 overruns Received 0 broadcasts, 0
multicast, 3955973016 unicast 0 runts, 0 giants, 0 jabbers 0 input errors, 0 CRC, 0 fragments,
 0 pause input 3955781430 packets output, 1598708166660 bytes, 0 underruns 0 broadcast, 0
multicast, 3955781430 unicast 0 late collisions, 0 collisions, 0 deferred 0 bad bytes
received, 0 multiple, 94987 pause output
```

The following example displays output for the **show platform mgf statistics cpu** command when entered on a Cisco 3945 ISR.

```
Router# show platform mgf statistics cpu
Backplane-GigabitEthernet0/3 is up, line protocol is up
  Hardware is PQ3_TSEC, address is 001b.5428.d403 (bia 001b.5428.d403)
  MTU 9600 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Full-duplex, 1000Mb/s, media type is internal
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out Interface statistics for CPU:
(port 0)
-----------------------------------------------------
30 second input rate 0 packets/sec
30 second output rate 0 packets/sec
0 packets input, 0 bytes, 0 overruns
Received 0 broadcasts, 0 multicast, 0 unicast 0 runts, 0 giants, 0 jabbers 0 input errors,
 0 CRC, 0 fragments, 0 pause input 0 packets output, 0 bytes, 0 underruns 0 broadcast, 0
multicast, 0 unicast 0 late collisions, 0 collisions, 0 deferred 0 bad bytes received, 0
multiple, 0 pause output
```

Related Commands

Command	Description
show platform	To display platform information, use the show platform command in privileged EXEC mode.

show platform resources

To display information about the utilization of platform resources, such as the Control Processor (CP), Service Processor (SP), DRAM, bootflash, and harddisk, use the **show platform resources** command in privileged EXEC mode.

The command now reports Control Processor (CP) and Service Processor (SP) CPU utilization under the 'Control/Service Processor' entry.

show platform resources {R0 | R0 cpu | R0 memory | exmem | datapath | datpath oversubscription}

Syntax Description

Table 215: Syntax Description

R0	Shows the CPU summary from a BINOS perspective.
R0 cpu	Shows the CPU utilization.
R0 memory	Shows the memory utilization.
exmem	Shows the user allocation statistics.
datapath	Shows the quantum flow processor utilization.
datapath oversubscription	Shows the oversubscription of the quantum flow processor.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE release 3.14	This command was introduced.
Cisco IOS XE Gibraltar 16.11.1	The command output is enhanced to include bootflash and harddisk information for Route Processors.
Cisco IOS XE Amsterdam 17.3.1	This command was modified. The following keywords were added: **R0**, **R0 cpu**, **R0 memory**, **exmem**, **datapath**, and **datapath oversubscription**.

Examples

The following sample output from the **show platform resources** command displays resource utilization related to the Embedded Service Processor and the Route Processor.

```
Router# show platform resources
**State Acronym: H - Healthy, W - Warning, C - Critical

Resource                 Usage                Max              Warning          Critical
     State
-------------------------------------------------------------------------------------------
RP0 (ok, active)
     H
 Control Processor       0.60%                100%             80%              90%
     H
  DRAM                   3077MB(40%)          7567MB           88%              93%
     H
  bootflash              3900MB(53%)          7305MB           88%              93%
```

```
    H
  harddisk             8223MB(8%)          93836MB        88%            93%
    H
RP1 (ok, standby)
    H
 Control Processor     0.00%               100%           80%            90%
    H
  DRAM                 2982MB(39%)         7567MB         88%            93%
    H
  bootflash            2564MB(35%)         7305MB         88%            93%
    H
  harddisk             14377MB(15%)        93836MB        88%            93%
    H
ESP0(ok, active)
    H
 Control Processor     0.60%               100%           80%            90%
    H
  DRAM                 1027MB(13%)         7872MB         88%            93%
    H
 QFP
    H
  TCAM                 240834cells(45%)    524288cells    65%            85%
    H
  DRAM                 181248KB(17%)       1048576KB      85%            95%
    H
  IRAM                 13013KB(9%)         131072KB       85%            95%
    H
  Pkt Buf Mem          55296KB(15%)        65535KB        85%            95%
    H
  CPU Utilization      0.00%               100%           90%            95%
    H
ESP1(ok, standby)
    H
 Control Processor     0.70%               100%           80%            90%
    H
  DRAM                 1016MB(12%)         7872MB         88%            93%
    H
 QFP
    H
  TCAM                 240834cells(45%)    524288cells    65%            85%
    H
  DRAM                 181248KB(17%)       1048576KB      85%            95%
    H
  IRAM                 13013KB(9%)         131072KB       85%            95%
    H
  CPU Utilization      0.00%               100%           90%            95%
    H
```

The output fields are self-explanatory.

Note On platforms where the harddisk is not present, only the bootflash information is displayed.

show platform slot r0 pcie status

To display information about all Peripheral Component Interconnect (PCI) buses on the Route Processor (RP) slot on the Cisco ASR 1000 Series Aggregation Services Router and devices connected to the PCI buses, use the **show platform slot r0 pcie status** command in user EXEC or privileged EXEC mode.

show platform slot r0 pcie status

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)
User EXEC (>)

Command History

Release	Modification
Cisco IOS XE Release 3.6	This command was introduced.

Examples

The following sample output from the **show platform slot r0 pcie status** command displays information about all PCI buses on the RP slot on the Cisco ASR 1000 Series Aggregation Services Router and the devices connected to them:

```
Router# show platform slot r0 pcie status

00:00.0 Class 0600: Device 8086:65c0 (rev 90)
00:02.0 Class 0604: Device 8086:65f7 (rev 90)
00:03.0 Class 0604: Device 8086:65e3 (rev 90)
00:04.0 Class 0604: Device 8086:65e4 (rev 90)
00:05.0 Class 0604: Device 8086:65e5 (rev 90)
00:06.0 Class 0604: Device 8086:65e6 (rev 90)
00:07.0 Class 0604: Device 8086:65e7 (rev 90)
00:08.0 Class 0880: Device 8086:65ff (rev 90)
00:10.0 Class 0600: Device 8086:65f0 (rev 90)
00:10.1 Class 0600: Device 8086:65f0 (rev 90)
00:10.2 Class 0600: Device 8086:65f0 (rev 90)
00:11.0 Class 0600: Device 8086:65f1 (rev 90)
00:13.0 Class 0600: Device 8086:65f3 (rev 90)
00:15.0 Class 0600: Device 8086:65f5 (rev 90)
00:16.0 Class 0600: Device 8086:65f6 (rev 90)
00:19.0 Class 0200: Device 8086:10e5 (rev 02)
00:1a.0 Class 0c03: Device 8086:2937 (rev 02)
00:1a.1 Class 0c03: Device 8086:2938 (rev 02)
00:1a.2 Class 0c03: Device 8086:2939 (rev 02)
00:1a.7 Class 0c03: Device 8086:293c (rev 02)
00:1b.0 Class 0403: Device 8086:293e (rev 02)
00:1d.0 Class 0c03: Device 8086:2934 (rev 02)
00:1d.1 Class 0c03: Device 8086:2935 (rev 02)
```

The output fields are self-explanatory.

show platform software agent iomd

To display the packets of High Priority and Low Priority queue in Over Subscription mode, use the **show platform software agent iomd** command in privileged EXEC mode.

show platform software agent iomd *im module* **dump fpga** *port number*

Syntax Description

im module	The name of the interface module.
port number	The port number used

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced on Cisco ASR 900 Series Routers and Cisco NCS 4200 Routers.

Examples

```
#show platform software agent iomd 0/8 dump fpga 4
OS LP Drop Q Pkt Cnt :0x0
OS HP Drop Q Pkt Cnt :0x0
OS LP Q Pkt Cnt :0x22906bd0
OS HP Q Pkt Cnt :0x55fdd731
```

To clear the High Priority and Low Priority counters in Over Subscription mode, use the **show platform software agent iomd** command in privileged EXEC mode.

show platform software agent iomd *im module* **clear fpga** *port number*

Syntax Description

im module	The name of the interface module.
port number	The port number used

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced on Cisco ASR 900 Series Routers and Cisco NCS 4200 Routers.

Examples

```
#show platform software agent iomd 0/8 clear fpga 4
OS LP Drop Q Pkt Cnt :0x0
OS HP Drop Q Pkt Cnt :0x0
```

```
OS LP Q Pkt Cnt :0x0
OS HP Q Pkt Cnt :0x0
```

show platform software audit

To display the SE Linux Audit logs, use the **show platform software audit** command in privileged EXEC mode.

show platform software audit { **all** | **summary** | **0** | **1** | **2** | **F0** | **R0** | **FP active** | **RP active**}

Syntax Description

all	Shows the audit log from all the slots.
summary	Shows the audit log summary count from all the slots.
0	Shows the audit log for the SM-Inter-Processor slot 0.
1	Shows the audit log for the SM-Inter-Processor slot 1.
2	Shows the audit log for the SM-Inter-Processor slot 2.
F0	Shows the audit log for the Embedded-Service-Processor slot 0.
R0	Shows the audit log for the Route-Processor slot 0.
FP active	Shows the audit log for the active Embedded-Service-Processor slot.
RP active	Shows the audit log for the active Route-Processor slot.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced on Cisco ISR 4000 series routers, Cisco CSR 1000V series routers, and Cisco 1000 ISR series routers running time-sensitive networking (TSN).

Usage Guidelines

This command was introduced in the Cisco IOS XE Gibraltar 16.11.1 as a part of the SELinux Permissive Mode feature. The **show platform software audit** command displays the system logs containing the access violation events.

In Cisco IOS XE Gibraltar 16.11.1, operation in a permissive mode is available - with the intent of confining specific components (process or application) of the IOS-XE platform. In the permissive mode, access violation events are detected and system logs are generated, but the event or operation itself is not blocked. The solution operates mainly in an access violation detection mode.

The following is a sample output of the `show software platform software audit summary` command:

```
Device# show platform software audit summary
===================================
AUDIT LOG ON ACTIVE
-----------------------------------
AVC Denial count: 7
```

The following is a sample output of the **show software platform software audit all** command. This command displays the information in the `audit.log` file.

```
Device#sh pla software audit all
===================================
AUDIT LOG ON ACTIVE
-----------------------------------
========== START ============
type=DAEMON_START msg=audit(1553837190.262:3031): op=start ver=2.6.6 format=raw kernel=4.4.172
 auid=4294967295 pid=446 subj=system_u:system_r:auditd_t:s0 res=success
type=NETFILTER_CFG msg=audit(1553837185.956:2): table=nat family=2 entries=0
type=MAC_STATUS msg=audit(1553837186.523:3): enforcing=1 old_enforcing=0 auid=4294967295
ses=4294967295
type=SYSCALL msg=audit(1553837186.523:3): arch=c000003e syscall=1 success=yes exit=1 a0=3
a1=7ffcf1c22070 a2=1 a3=0 items=0 ppid=203 pid=205 auid=4294967295 uid=0 gid=0 euid=0 suid=0
 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="load_policy"
exe="/usr/sbin/load_policy" subj=kernel key=(null)
type=PROCTITLE msg=audit(1553837186.523:3):
proctitle=2F7573722F7362696E2F6C6F61645F706F6C696379002D69
type=MAC_POLICY_LOAD msg=audit(1553837186.528:4): policy loaded auid=4294967295 ses=4294967295
type=SYSCALL msg=audit(1553837186.528:4): arch=c000003e syscall=1 success=yes exit=1693637
 a0=4 a1=7f792d1d6000 a2=19d7c5 a3=f items=0 ppid=203 pid=205 auid=4294967295 uid=0 gid=0
euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="load_policy"
exe="/usr/sbin/load_policy" subj=system_u:system_r:kernel_t:s0 key=(null)
…
```

You can use the output of this command to copy the contents of `audit.log` to a file to then transfer to a remote host.

```
Device#show platform software audit all | redirect bootflash:audi_123.log

Device#dir bootflash:audi_123.log
Directory of bootflash:/audi_123.log
   27  -rw-           35305  Mar 29 2019 22:16:36 +00:00  audi_123.log

3249049600 bytes total (538112000 bytes free)
```

show platform software memory

To display memory information for the specified process, use the **show platform software memory**command in privileged EXEC or diagnostic mode.

show platform software memory [{**database** | **messaging**}]{**chassis-manager** *slot* | **cpp-control-process** *process* | **cpp-driver** *process* | **cpp-ha-server** *process* | **cpp-service-process** *process* | **forwarding-manager** *slot* | **host-manager** *slot* | **interface-manager** *slot* | **ios** *slot* | **logger** *slot* | **pluggable-services** *slot* | **shell-manager** *slot*} [**brief**]

Syntax Description

database database	(Optional) Displays database memory information for the specified process.
messaging	(Optional) Displays messaging memory information for specified process. The information displayed is for internal debugging purposes only.
chassis-manager *slot*	Displays memory information for the Chassis Manager process in the specified *slot*. Possible *slot* values are: • **0** --Cisco ASR 1000 Series SPA Interface Processor (SIP) slot 0 • **1** --Cisco ASR 1000 Series SIP slot 1 • **2** --Cisco ASR 1000 Series SIP slot 2 • **f0** --Cisco ASR 1000 Series Embedded Services Processor (ESP) slot 0 • **f1** --Cisco ASR 1000 Series ESP slot 1 • **fp active** --Active Cisco ASR 1000 Series ESP • **fp standby** --Standby Cisco ASR 1000 Series ESP • **r0** --Cisco ASR 1000 Series Route Processor (RP) slot 0 • **r1** --Cisco ASR 1000 Series RP slot 1 • **rp active** --Active Cisco ASR 1000 Series RP • **rp standby** --Standby Cisco ASR 1000 Series RP
cpp-control-process	Displays memory information for the specified Cisco Packet Processor (CPP) Client Control process. Possible *process* values are: • **cpp active** --Active CPP Client Control process • **cpp standby** --Standby CPP Client Control process The information displayed is for internal debugging purposes only.

cpp-driver	Displays memory information for the specified CPP Driver process. Possible *process* values are: • **cpp active** --Active CPPDriver process • **cpp standby** --Standby CPP Driver process The information displayed is for internal debugging purposes only.
cpp-ha-server	Displays memory information for the specified CPP High Availability (HA) Server process. Possible *process* values are: • **cpp active** --Active CPP HA Server process • **cpp standby** --Standby CPP HA Server process The information displayed is for internal debugging purposes only.
cpp-service-process	Displays memory information for the specified CPP Client Service process. Possible *process* values are: • **cpp active** --Active CPP Client Service process • **cpp standby** --Standby CPP Client Service process The information displayed is for internal debugging purposes only.
forwarding-manager *slot*	Displays memory information for the Forwarding Manager process in the specified *slot*. Possible *slot* values are: • **f0** --Cisco ASR 1000 Series ESP slot 0 • **f1** --Cisco ASR 1000 Series ESP slot 1 • **fp active** --Active Cisco ASR 1000 Series ESP • **fp standby** --Standby Cisco ASR 1000 Series ESP • **r0** --Cisco ASR 1000 Series RP slot 0 • **r1** --Cisco ASR 1000 Series RP slot 1 • **rp active** --Active Cisco ASR 1000 Series RP • **rp standby** --Standby Cisco ASR 1000 Series RP

host-manager *slot*	Displays memory information for the Host Manager process in the specified *slot*. Possible *slot* values are: • **0** --Cisco ASR 1000 Series SIP slot 0 • **1** --Cisco ASR 1000 Series SIP slot 1 • **2** --Cisco ASR 1000 Series SIP slot 2 • **f0** --Cisco ASR 1000 Series ESP slot 0 • **f1** --Cisco ASR 1000 Series ESP slot 1 • **fp active** --Active Cisco ASR 1000 Series ESP • **fp standby** --Standby Cisco ASR 1000 Series ESP • **r0** --Cisco ASR 1000 Series RP slot 0 • **r1** --Cisco ASR 1000 Series RP slot 1 • **rp active** --Active Cisco ASR 1000 Series RP • **rp standby** --Standby Cisco ASR 1000 Series RP
interface-manager *slot*	Displays memory information for the Interface Manager process in the specified *slot*. Possible *slot* values are: • **0** --Cisco ASR 1000 Series SIP slot 0 • **1** --Cisco ASR 1000 Series SIP slot 1 • **2** -- Cisco ASR 1000 Series SIP slot 2 • **r0** --Cisco ASR 1000 Series RP slot 0 • **r1** --Cisco ASR 1000 Series RP slot 1 • **rp active** --Active Cisco ASR 1000 Series RP • **rp standby** --Standby Cisco ASR 1000 Series RP

ios *slot*	Displays memory information for the IOS process in the specified *slot*. Possible *slot* values are: • **0/0** --Cisco ASR 1000 Series SIP slot 0, bay 0 • **0/1** --Cisco ASR 1000 Series SIP slot 0, bay 1 • **0/2** --Cisco ASR 1000 Series SIP slot 0, bay 2 • **0/3** --Cisco ASR 1000 Series SIP slot 0, bay 3 • **1/0** --Cisco ASR 1000 Series SIP slot 1, bay 0 • **1/1** --Cisco ASR 1000 Series SIP slot 1, bay 1 • **1/2** --Cisco ASR 1000 Series SIP slot 1, bay 2 • **1/3** --Cisco ASR 1000 Series SIP slot 1, bay 3 • **2/0** --Cisco ASR 1000 Series SIP slot 2, bay 0 • **2/1** --Cisco ASR 1000 Series SIP slot 2, bay 1 • **2/2** --Cisco ASR 1000 Series SIP slot 2, bay 2 • **2/3** --Cisco ASR 1000 Series SIP slot 2, bay 3 • **r0** --Cisco ASR 1000 Series RP slot 0 • **r1** --Cisco ASR 1000 Series RP slot 1 • **rp active** --Active Cisco ASR 1000 Series RP • **rp standby** --Standby Cisco ASR 1000 Series RP
logger *slot*	Displays memory information for the logger process in the specified *slot*. Possible *slot* values are: • **0** --Cisco ASR 1000 Series SIP slot 0 • **1** --Cisco ASR 1000 Series SIP slot 1 • **2** --Cisco ASR 1000 Series SIP slot 2 • **f0** --Cisco ASR 1000 Series ESP slot 0 • **f1** --Cisco ASR 1000 Series ESP slot 1 • **fp active** --Active Cisco ASR 1000 Series ESP • **fp standby** --Standby Cisco ASR 1000 Series ESP • **r0** --Cisco ASR 1000 Series RP slot 0 • **r1** --Cisco ASR 1000 Series RP slot 1 • **rp active** --Active Cisco ASR 1000 Series RP • **rp standby** --Standby Cisco ASR 1000 Series RP

pluggable-services *slot*	Displays memory information for the pluggable-services process in the specified *slot*. Possible *slot* values are: • **r0** --Cisco ASR 1000 Series RP slot 0 • **r1** --Cisco ASR 1000 Series RP slot 1 • **rp active** --Active Cisco ASR 1000 Series RP • **rp standby** --Standby Cisco ASR 1000 Series RP
shell-manager *slot*	Displays memory information for the Shell Manager process in the specified slot. Possible *slot* values are: • **r0** --Cisco ASR 1000 Series RP slot 0 • **r1** --Cisco ASR 1000 Series RP slot 1 • **rp active** --Active Cisco ASR 1000 Series RP • **rp standby** --Standby Cisco ASR 1000 Series RP
brief	(Optional) Displays abbreviated memory information for the specified process.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Diagnostic (diag)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines

The specification of the database and brief keywords are optional.

The specification of a process and slot are required.

Examples

The following example displays memory information for the Forwarding Manager process for Cisco ASR 1000 Series RP slot 0:

```
Router# show platform software memory forwarding-manager r0
Module: cdllib
  allocated: 900, requested: 892, overhead: 8
  Allocations: 2, failed: 0, frees: 1
Module: eventutil
  allocated: 117379, requested: 117059, overhead: 320
  Allocations: 46, failed: 0, frees: 6
Module: uipeer
  allocated: 9264, requested: 9248, overhead: 16
  Allocations: 3, failed: 0, frees: 1
Module: Summary
  allocated: 127543, requested: 127199, overhead: 344
  Allocations: 51, failed: 0, frees: 8
```

The table below describes the significant fields shown in the display.

Table 216: show platform software memory Field Descriptions

Field	Description
Module:	Name of submodule.
allocated:	Memory, allocated in bytes.
requested:	Number of bytes requested by application.
overhead:	Allocation overhead.
Allocations:	Number of discrete allocation event attempts.
failed:	Number of allocation attempts that were attempted, but failed.
frees:	Number of free events.

The following example displays abbreviated (brief keyword) memory information for the Chassis Manager process for Cisco ASR 1000 Series ESP slot 0:

```
Router# show platform software memory chassis-manager f0 brief

  module            allocated     requested     allocs        frees
  ------------------------------------------------------------------------
  CPP Features      692           668           3             0
  Summary           497816        495344        323           14
  chunk             419322        419290        4             0
  eventutil         68546         66146         312           12
  uipeer            9256          9240          4             2
```

The table below describes the significant fields shown in the **brief** keyword display.

Table 217: show platform software memory brief Field Descriptions

Field	Description
module	Name of submodule.
allocated	Memory, allocated in bytes.
requested	Number of bytes requested by application.
allocs	Number of discrete allocation event attempts.
frees	Number of free events.

show platform software mount

To display the mounted file systems, both physical and virtual, for a Cisco ASR 1000 Series SPA Interface Processor (SIP), Cisco ASR 1000 Series Embedded Services Processor (ESP), or Cisco ASR 1000 Series Route Processor (RP), use the **show platform software mount**command in privileged EXEC or diagnostic mode.

show platform software mount [*slot* [**brief**]]

Syntax Description

slot	(Optional) Displays mounted file systems for the specified *slot*. Possible *slot* values are: • **0** --Cisco ASR 1000 Series SIP slot 0 • **1** --Cisco ASR 1000 Series SIP slot 1 • **2** --Cisco ASR 1000 Series SIP slot 2 • **f0** --Cisco ASR 1000 Series ESP slot 0 • **f1** --Cisco ASR 1000 Series ESP slot 1 • **fp active** --Active Cisco ASR 1000 Series ESP • **fp standby** --Standby Cisco ASR 1000 Series ESP • **r0** --Cisco ASR 1000 Series RP slot 0 • **r1** --Cisco ASR 1000 Series RP slot 1 • **rp active** --Active Cisco ASR 1000 Series RP • **rp standby** --Standby Cisco ASR 1000 Series RP
brief	(Optional) Displays abbreviated mounted file system information.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Diagnostic (diag)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines

If no slot is specified, the command returns mounted file systems for the active RP.

This command allows you to ascertain the presence or absence of specific system mounts. For example, this command might be used to determine /tmp-related mounts, which are used to create many run-time directories and files.

Users may be requested to execute this command to collect information about the underlying configuration of the platform software.

The RP output can differ depending on how the router was booted, and whether there are USB devices inserted.

The SIP and ESP output can differ depending on whether the chassis is a dual or single RP.

Examples

The following example displays mounted file systems for the active RP:

```
Router# show platform software mount
Filesystem                         Used   Available  Use% Mounted on
rootfs                                0           0     - /
proc                                  0           0     - /proc
sysfs                                 0           0     - /sys
none                                524     1037640    1% /dev
/dev/bootflash1                  298263       42410   88% /bootflash
/dev/harddisk1                   609208     4025132   14% /misc/scratch
/dev/loop1                        28010           0  100% /tmp/sw/mount/2007-10-14_...
/dev/loop2                        26920           0  100% /tmp/sw/mount/2007-10-14_...
/dev/loop3                        48236           0  100% /tmp/sw/mount/2007-10-14_...
/dev/loop4                         6134           0  100% /tmp/sw/mount/2007-10-14_...
/dev/loop5                        43386           0  100% /tmp/sw/mount/2007-10-14_...
/dev/loop6                        30498           0  100% /tmp/sw/mount/2007-10-14_...
/dev/loop7                        14082           0  100% /tmp/sw/mount/2007-10-14_...
none                                524     1037640    1% /dev
/proc/bus/usb                         0           0     - /proc/bus/usb
/dev/mtdblock1                      460        1588   23% /obfl
automount(pid4165)                    0           0     - /vol
```

The following example displays mounted file systems for the Cisco ASR 1000 Series ESP in ESP slot 0:

```
Router# show platform software mount f0
Filesystem                         Used   Available Use% Mounted on
rootfs                                0           0     - /
proc                                  0           0     - /proc
sysfs                                 0           0     - /sys
none                              10864      507124    3% /dev
/dev/loop1                        41418           0  100% /tmp/sw/fp/0/0/fp/mount
none                              10864      507124    3% /dev
/proc/bus/usb                         0           0     - /proc/bus/usb
/dev/mtdblock1                      504        1544   25% /obfl
automount(pid3210)                    0           0     - /misc1
```

The following example displays mounted file systems for the active Cisco ASR 1000 Series RP:

```
Router# show platform software mount rp active
Filesystem                         Used   Available  Use% Mounted on
rootfs                                0           0     - /
proc                                  0           0     - /proc
sysfs                                 0           0     - /sys
none                                436     1037728    1% /dev
/dev/bootflash1                  256809       83864   76% /bootflash
/dev/harddisk1                   252112     4382228    6% /misc/scratch
/dev/loop1                        30348           0  100% /tmp/sw/mount/2007-09-27_...
/dev/loop2                        28394           0  100% /tmp/sw/mount/2007-09-27_...
/dev/loop3                        42062           0  100% /tmp/sw/mount/2007-09-27_...
/dev/loop4                         8384           0  100% /tmp/sw/mount/2007-09-27_...
/dev/loop5                        41418           0  100% /tmp/sw/mount/2007-09-27_...
/dev/loop6                        21612           0  100% /tmp/sw/mount/2007-09-27_...
/dev/loop7                        16200           0  100% /tmp/sw/mount/2007-09-27_...
none                                436     1037728    1% /dev
/proc/bus/usb                         0           0     - /proc/bus/usb
```

```
/dev/mtdblock1                          484         1564   24%  /obfl
automount(pid4004)                        0            0     -  /vol
```

The table below describes the significant fields shown in the SIP slot (0, 1, or 2) displays.

Table 218: show platform software mount SIP slot Field Descriptions

Field	Description
Filesystem	Logical name of the file system device.
Used	Number of 1Kb blocks used.
Available	Number of free 1Kb blocks available.
Use%	Percentage of 1Kb blocks used of the total available.
Mounted on	Canonical path to the mounted file system.

The following example displays abbreviated (brief keyword) mounted file system information for Cisco ASR 1000 Series SIP slot 0:

```
Router# show platform software mount 0 brief
Mount point: rootfs
  Type     : rootfs
  Location : /
  Options  : rw
Mount point: proc
  Type     : proc
  Location : /proc
  Options  : rw
Mount point: sysfs
  Type     : sysfs
  Location : /sys
  Options  : rw
Mount point: none
  Type     : tmpfs
  Location : /dev
  Options  : rw
Mount point: /dev/loop1
  Type     : iso9660
  Location : /tmp/sw/cc/0/0/cc/mount
  Options  : ro

Mount point: none
  Type     : tmpfs
  Location : /dev
  Options  : rw

Mount point: /proc/bus/usb
  Type     : usbfs
  Location : /proc/bus/usb
  Options  : rw

Mount point: /dev/mtdblock1
  Type     : jffs2
  Location : /obfl
  Options  : rw,noatime,nodiratime

Mount point: automount(pid3199)
  Type     : autofs
```

```
Location : /misc1
Options  : rw,fd=5,pgrp=3199,timeout=60,minproto=2,maxproto=4,indirect
```

The tab le below describes the significant fields shown in the brief keyword display.

Table 219: show platform software mount brief Field Descriptions

Field	Description
Mount point:	Logical name of the file system device.
Type:	File system type.
Location:	Canonical path to the mounted file system.
Options:	Mount point type-specific flags and settings.

show platform software infrastructure punt-keepalive

To display information about the settings for the **platform punt-keepalive** command, use the **show platform software infrastructure punt-keepalive** command in the privileged EXEC mode.

show platform software infrastructure punt-keepalive

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.

Examples

The following is a sample output of the **show platform software infrastructure punt-keepalive** command when the punt-keepalive feature is enabled:

```
Router# show platform software infrastructure punt-keepalive

----- punt inject keepalive settings -----
punt keepalive interval (sec) = 2
punt keepalive warn count(miss) = 10
punt keepalive fatal (warn count) = 15

----- punt inject keepalive status -----
Last punt keepalive proc sched = 1.140 sec ago
Last punt keepalive sent = 1.140 sec ago
punt keepalive rx count = 1473
punt keepalive tx count = 1473
punt keepalive last keepalive received = yes

----- punt inject keepalive errors -----
punt keepalive failed to send no buffers = 0
punt keepalive tx fail count = 0

----- punt inject keepalive tweaks -----
ignore rx keepalive msg = no
ignore keepalive failover fault = yes
```

The following is a sample output of the **show platform software infrastructure punt-keepalive** command when the punt-keepalive feature is disabled:

```
Router# show platform software infrastructure punt-keepalive

----- punt inject keepalive settings -----
punt keepalive fatal (warn count) = 15
punt keepalive interval (sec) = 0(Stopped)
punt keepalive warning count (miss) = 10
Disable XE kernel core = No

----- punt inject keepalive status -----
```

```
Last punt keepalive proc sched = 8.005 sec ago
Last punt keepalive sent = 8.195 sec ago
punt keepalive rx count = 6695
punt keepalive tx count = 6695
punt keepalive last keepalive received = yes

----- punt inject keepalive errors -----
punt keepalive failed to send no buffers = 0
punt keepalive tx fail count = 0
```

Related Commands

Command	Description
platform punt-keepalive	Enables the Punt-Keepalive feature and monitors the status of the punt path between the forwarding processor (FP) and the route processor (RP).

show platform software interface summary

To display a summary of statistics for interfaces that are configured on a networking device, use the **show platform software interface summary** command in privileged EXEC mode.

show platform software interface summary [{[*name*][*queues*][*rates*]}]

Syntax Description

name	(Optional) Displays, for the named interface, a summary of the packets held and dropped in input/output queues and the transmission/reception rates.
queues	(Optional) Displays a summary of the packets held and dropped in input/output queues, for interfaces on the router..
rates	(Optional) Displays a summary of the transmission/reception rates, for interfaces on the router.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9	This command was introduced on Cisco 4400 Series Routers.

Usage Guidelines

Cisco ISR 4400 Series

On a Cisco ISR 4400 Series router you can use this command to show a summary of the packets held and dropped in input/output queues and the transmit/receive rates, for interfaces on the router.

Examples

The following example displays summary information for the interfaces of a Cisco 4400 Series router.

```
Router# show platform software interface summary
 Interface                  IHQ  IQD  OHQ  OQD  RXBS  RXPS  TXBS  TXPS  TRTL
-----------------------------------------------------------------------------
  GigabitEthernet0/0/0        0    0    0    0     0     0     0     0     0
  GigabitEthernet0/0/1        0    0    0    0     0     0     0     0     0
  GigabitEthernet0/0/2        0    0    0    0     0     0     0     0     0
  GigabitEthernet0/0/3        0    0    0    0     0     0     0     0     0
  Serial1/0/0                 0    0    0    0     0     0     0     0     0
* GigabitEthernet0            0    0    0    0 34000    60     0     0     0
```

Table 220: show platform software interface summary Field Descriptions

Field	Description
IHQ	Packets in input hold queue.
IQD	Packets dropped from input queue.
OHQ	Packets in output hold queue.

Field	Description
OQD	Packets dropped from output queue.
RXBS	Reception rate in bits per second.
RXPS	Reception rate in packets per second.
TXBS	Transmission rate in bits per second.
TXPS	Transmission rate in packets per second.
TRTL	Throttle count.

The following example displays summary (queues) information for interfaces of a Cisco 4400 Series router.

```
Router# show platform software interface summary queues

Interface                      IHQ           IQD           OHQ           OQD
----------------------------------------------------------------------------
GigabitEthernet0/0/0             0             0             0             0
GigabitEthernet0/0/1             0             0             0             0
GigabitEthernet0/0/2             0             0             0             0
GigabitEthernet0/0/3             0             0             0             0
Serial1/0/0                      0             0             0             0
GigabitEthernet0                 0             0             0             0
```

The table below describes the significant fields shown in the queues keyword display.

Table 221: show platform software interface summary queues Field Descriptions

Field	Description
IHQ	Packets in input hold queue.
IQD	Packets dropped from input queue.
OHQ	Packets in output hold queue.
OQD	Packets dropped from output queue.

Related Commands

Command	Description
show interfaces summary	Displays a summary of statistics for interfaces on a networking device.

show platform software l2pt statistics

Network devices maintain statistics counters for performance monitoring. Statistics counters in the Cisco routers collect Layer 2 Protocol Tunneling (L2PT) statistics, such as the number of packets that are enqueued and dequeued to an L2PT process, packets dropped, total number of outgoing tunneled packets, total number of outgoing L2 control packets, and unprocessed packets. Use the **show platform software l2pt statistics** command in previleged EXEC mode to collect L2PT statistics.

show platform software l2pt statistics

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Release	Modification
Cisco IOS XE Dublin 17.10.1	This command was introduced on Cisco NCS 520 Series Routers.

Examples

```
Router#show platform software l2pt statistics
Platform L2PT statistics:
 Number of packets enqueued to L2PT process  : 36
 Number of packets dequeued from L2PT process: 36
 Number of packets dropped                   : 0
 Total number of tunneled packets out        : 72
 Total number of L2 control packets out      : 0
 Number of packets failed to process         : 0
```

clear platform software l2pt counters

The **clear platform software l2pt counters** command clears the Layer 2 Protocol Tunneling (L2PT) statistics collected by the statistics counters.

clear platform software l2pt counters

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Release	Modification
Cisco IOS XE Dublin 17.10.1	This command was introduced on Cisco NCS 520 Series Routers.

Examples

```
Router#clear pla software l2pt counters
RTR1-Dom2#sh pla software l2pt statistics
Platform L2PT statistics:
 Number of packets enqueued to L2PT process  : 0
 Number of packets dequeued from L2PT process: 0
 Number of packets dropped                   : 0
 Total number of tunneled packets out        : 0
```

```
Total number of L2 control packets out      : 0
Number of packets failed to process         : 0
```

show platform software process list

To display a list of the processes running in a given slot, use the **show platform software process list**command in privileged EXEC or diagnostic mode.

show platform software process list *slot* [{**name** *process-name* | **process-id** *process-id* | **sort** *memory* | **summary**}]

Syntax Description

slot	Displays running process information for the specified *slot*. Possible *slot* values are: • **0**--Cisco ASR 1000 Series SPA Interface Processor (SIP) slot 0 • **1**--Cisco ASR 1000 Series SIP slot 1 • **2**--Cisco ASR 1000 Series SIP slot 2 • **f0**--Cisco ASR 1000 Series Embedded Services Processor (ESP) slot 0 • **f1**--Cisco ASR 1000 Series ESP slot 1 • **fp active**--Active Cisco ASR 1000 Series ESP • **fp standby**--Standby Cisco ASR 1000 Series ESP • **r0**--Cisco ASR 1000 Series Route Processor (RP) slot 0 • **r1**--Cisco ASR 1000 Series RP slot 1 • **rp active**--Active Cisco ASR 1000 Series RP • **rp standby**--Standby Cisco ASR 1000 Series RP
name *process-name*	(Optional) Displays information for the specified process name.
process-id process-id	(Optional) Displays information for the specified process ID.
sort *memory*	(Optional) Sorts the processes by memory.
summary	(Optional) Displays summary process information for the running host.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Diagnostic (diag)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines

The name and process-id keywords can be used to narrow the process list display down to specific processes.

The **sort** keyword can be used to sort the process list by memory size.

The summary keyword can be used to display summary information about running processes.

Examples

The following example displays information about running processes for Cisco ASR 1000 Series SIP slot 0:

```
Router# show platform software process list 0

Name                     Pid    PPid  Group Id  Status    Priority  Size
------------------------------------------------------------------------------
init                       1       0         1  S               20  1974272
ksoftirqd/0                2       1         1  S               39  0
events/0                   3       1         1  S               15  0
khelper                    4       1         1  S               15  0
kthread                    5       1         1  S               15  0
kblockd/0                 19       5         1  S               15  0
khubd                     23       5         1  S               15  0
pdflush                   59       5         1  S               20  0
pdflush                   60       5         1  S               20  0
kswapd0                   61       5         1  S               15  0
aio/0                     62       5         1  S               15  0
xfslogd/0                 63       5         1  S               15  0
xfsdatad/0                64       5         1  S               15  0
mtdblockd                626       1         1  S               20  0
loop0                   1370       1         1  S                0  0
portmap                 1404       1      1404  S               20  2076672
portmap                 1406       1      1406  S               20  2076672
loop1                   1440       1         1  S                0  0
udevd                   2104       1      2104  S               16  1974272
jffs2_gcd_mtd1          2796       1         1  S               30  0
klogd                   3093       1      3093  S               20  1728512
automount               3199       1      3199  S               20  2396160
xinetd                  3214       1      3214  S               20  3026944
xinetd                  3216       1      3216  S               20  3026944
pvp.sh                  3540       1      3540  S               20  3678208
inotifywait             3575    3540      3575  S               20  1900544
pman.sh                 3614    3540      3614  S               20  3571712
pman.sh                 3714    3540      3714  S               20  3571712
btrace_rotate.s         3721    3614      3721  S               20  3133440
agetty                  3822       1      3822  S               20  1720320
mcp_chvrf.sh            3823       1      3823  S               20  2990080
sntp                    3824       1      3824  S               20  2625536
issu_switchover         3825       1      3825  S               20  3899392
xinetd                  3827    3823      3823  S               20  3026944
cmcc                    3862    3714      3862  S               20  26710016
pman.sh                 3883    3540      3883  S               20  3571712
pman.sh                 4014    3540      4014  S               20  3575808
hman                    4020    3883      4020  R               20  19615744
imccd                   4114    4014      4114  S               20  31539200
inotifywait             4196    3825      3825  S               20  1896448
pman.sh                 4351    3540      4351  S               20  3575808
plogd                   4492    4351      4492  S               20  22663168
inotifywait             4604    3721      4604  S               20  1900544
```

The table below describes the significant fields shown in the display.

Table 222: show platform software process list Field Descriptions

Field	Description
Name	Name of the process.

Field	Description
Pid	Process ID.
PPid	Parent Process ID.
Group Id	Process group ID.
Status	Process status.
Priority	Process priority.
Size	Virtual memory size (in bytes).

The following example displays information about a specific named process for Cisco ASR 1000 Series SIP slot 0:

```
Router# show platform software process list 0 name sleep
Name: sleep
  Process id       : 25938
  Parent process id: 3891
  Group id         : 3891
  Status           : S
  Session id       : 3816
  User time        : 0
  Kernel time      : 0
  Priority         : 20
  Virtual bytes    : 2482176
  Resident pages   : 119
  Resident limit   : 4294967295
  Minor page faults: 182
  Major page faults: 0
```

The following example displays information about a specific process identifier for Cisco ASR 1000 Series SIP slot 0:

```
Router# show platform software process list 0 process-id 1

Name: init
  Process id       : 1
  Parent process id: 0
  Group id         : 1
  Status           : S
  Session id       : 1
  User time        : 1
  Kernel time      : 741
  Priority         : 20
  Virtual bytes    : 1974272
  Resident pages   : 161
  Resident limit   : 4294967295
  Minor page faults: 756
  Major page faults: 0
```

The table below describes the significant fields shown in the **name** and **process-id keyword**displays.

Table 223: show platform software process list name and process-id Field Descriptions

Field	Description
Name	Name of the process.
Process id	Process ID.
Parent process id	Parent process ID.
Group id	Process group ID.
Status	Process status.
Session id	Process session ID.
User time	Time (in seconds) spent in user mode.
Kernel time	Time (in seconds) spent in kernel mode.
Priority	Process priority.
Virtual bytes	Virtual memory size (in bytes).
Resident pages	Resident page size.
Resident limit	Current limit on Resident pages.
Minor page faults	Number of minor page faults.
Major page faults	Number of major page faults.

The following example displays process summary information for Cisco ASR 1000 Series SIP slot 0:

```
Router# show platform software process list 0 summary
Total number of processes: 54
  Running          : 4
  Sleeping         : 50
  Disk sleeping    : 0
  Zombies          : 0
  Stopped          : 0
  Paging           : 0
  Up time          : 1562
  Idle time        : 1511
  User time        : 1606
  Kernel time      : 1319
  Virtual memory   : 587894784
  Pages resident   : 45436
  Major page faults: 25
  Minor page faults: 149098
Architecture     : ppc
  Memory (kB)
    Physical       : 524288
    Total          : 479868
    Used           : 434948
    Free           : 44920
    Active         : 183020
    Inactive       : 163268
```

```
    Inact-dirty    : 0
    Inact-clean    : 0
    Dirty          : 0
    AnonPages      : 76380
    Bounce         : 0
    Cached         : 263764
    Commit Limit   : 239932
    Committed As   : 201452
    High Total     : 0
    High Free      : 0
    Low Total      : 479868
    Low Free       : 44920
    Mapped         : 59996
    NFS Unstable   : 0
    Page Tables    : 1524
    Slab           : 73760
    VMmalloc Chunk : 426840
    VMmalloc Total : 474856
    VMmalloc Used  : 47372
    Writeback      : 0
  Swap (kB)
    Total          : 0
    Used           : 0
    Free           : 0
    Cached         : 0
  Buffers (kB)     : 6144
  Load Average
    1-Min          : 0.00
    5-Min          : 0.00
    15-Min         : 0.00
```

The table below describes the significant fields shown in the **summary** keyword display.

Table 224: show platform software process list summary Field Descriptions

Field	Description
Total number of processes	Total number of processes in all possible states.
Running	Number of processes in the running state.
Sleeping	Number of processes in the sleeping state.
Disk sleeping	Number of processes in the disk-sleeping state.
Zombies	Number of processes in the zombie state.
Stopped	Number of processes in the stopped state.
Paging	Number of processes in the paging state.
Up time	System Up time (in seconds).
Idle time	System Idle time (in seconds).
User time	System time (in seconds) spent in user mode.
Kernel time	System time (in seconds) spent in kernel mode.
Virtual memory	Virtual memory size (in bytes).

Field	Description
Pages resident	Resident page size.
Major page faults	Number of major page faults.
Minor page faults	Number of minor page faults.
Architecture	System CPU architecture: PowerPC (ppc).
Memory (kB)	System memory heading.
Physical	Total physical memory (in kilobytes).
Total	Total available memory (in kilobytes). This value represents the physical memory available for kernel use.
Used	Used memory (in kilobytes).
Free	Free memory (in kilobytes).
Active	Most recently used memory (in kilobytes).
Inactive	Memory (in kilobytes) that has been less recently used. It is more eligible to be reclaimed for other purposes.
Inact-dirty	Memory (in kilobytes) that may need to be written to persistent store (cache or disk).
Inact-clean	Memory (in kilobytes) that is readily available for re-use.
Dirty	Memory (in kilobytes) that is waiting to get written back to the disk.
AnonPages	Memory (in kilobytes) that is allocated when a process requests memory from the kernel via the malloc() system call. This memory has no file backing on disk.
Bounce	Memory (in kilobytes) that is allocated to bounce buffers.
Cached	Amount of physical RAM (in kilobytes) used as cache memory.
Commit Limit	Total amount of memory (in kilobytes) currently available to be allocated on the system. This limit is only adhered to if strict overcommit accounting is enabled.
Committed As	Total amount of memory (in kilobytes) presently allocated on the system. The committed memory is a sum of all of the memory that has been allocated by processes, even if it has not been used by them as of yet.
High Total	Total amount of memory (in kilobytes) that is not directly mapped into kernel space. The High Total value can vary based on the type of kernel used.
High Free	Amount of free memory (in kilobytes) that is not directly mapped into kernel space. The High Free value can vary based on the type of kernel used.

Field	Description
Low Total	Total amount of memory (in kilobytes) that is directly mapped into kernel space. The Low Total value can vary based on the type of kernel used.
Low Free	Amount of free memory (in kilobytes) that is directly mapped into kernel space. The Low Free value can vary based on the type of kernel used.
Mapped	Total amount of memory (in kilobytes) that has been used to map devices, files, or libraries using the mmap command.
NFS Unstable	Total amount of memory (in kilobytes) used for unstable NFS pages. Unstable NFS pages are pages that have been written into the page cache on the server, but have not yet been synchronized to disk.
Page Tables	Total amount of memory (in kilobytes) dedicated to the lowest page table level.
Slab	Total amount of memory (in kilobytes) used by the kernel to cache data structures for its own use.
VMalloc Chunk	Largest contiguous block of available virtual address space (in kilobytes) that is free.
VMalloc Total	Total amount of memory (in kilobytes) of total allocated virtual address space.
VMalloc Used	Total amount of memory (in kilobytes) of used virtual address space.
Writeback	Memory (in kilobytes) that is actively being written back to the disk.
Swap (kB)	Swap memory heading.
Total	Total swap memory (in kilobytes).
Used	Used swap memory (in kilobytes).
Free	Free swap memory (in kilobytes).
Cached	Cached swap memory (in kilobytes).
Buffers (kB)	Buffers heading.
Load Average	Indicators of system load.
1-Min	Average number of processes running for the last minute.
5-Min	Average number of processes running for the last 5 minutes.
15-Min	Average number of processes running for the last 15 minutes.

The following example displays process summary information for Cisco ASR 1000 Series sorted by memory size:

```
Router#show platform software process list R0 sort memory
Name                         Pid    PPid  Group Id  Status    Priority  Size
------------------------------------------------------------------------------
linux_iosd-imag        27982   26696     27982  S               20  4294967295
```

```
fman_rp              25857  25309    25857  S             20  684867584
vman                 30685  29587    30685  S             20  194850816
smand                30494  28948    30494  S             20  103538688
libvirtd              5260   5254     5254  S             20  83197952
python               10234  10233    10210  S             20  29765632
python               10975  10234    10975  S             20  29765632
python               10977  10234    10977  S             20  29765632
python               10978  10234    10978  S             20  29765632
python               10979  10234    10979  S             20  29765632
python               10981  10234    10981  S             20  29765632
automount            15682      1    15682  S             20  25092096
cmand                25530  24760    25530  S             20  23789568
imand                27198  26090    27198  S             20  22040576
psd                  31284  28535    31284  S             20  16019456
emd                  25712  24917    25712  S             20  15302656
hman                 26622  25617    26622  R             20  14544896
plogd                28878  27718    28878  S             20  12349440
btrace_rotate.s      25251  24643    25251  S             20  6008832
sort_files_by_i      30092  29066    30092  S             20  5234688
periodic.sh          28469  27490    28469  S             20  4812800
rotee                 5403      1     5396  S             20  4788224
rotee                 5412      1     5411  S             20  4788224
rotee                 5438      1     5437  S             20  4788224
rotee                 5482      1     5481  S             20  4788224
rotee                 9844      1     9843  S             20  4788224
rotee                 9958      1     9957  S             20  4788224
rotee                16942      1    16941  S             20  4788224
rotee                16946      1    16945  S             20  4788224
rotee                24383      1    24382  S             20  4788224
rotee                24742      1    24741  S             20  4788224
rotee                24960      1    24959  S             20  4788224
rotee                25107      1    25106  S             20  4788224
rotee                25534      1    25533  S             20  4788224
rotee                25542      1    25541  S             20  4788224
rotee                25880      1    25879  S             20  4788224
rotee                26390      1    26389  S             20  4788224
rotee                26881      1    26880  S             20  4788224
rotee                27728      1    27727  S             20  4788224
rotee                27882      1    27881  S             20  4788224
rotee                28867      1    28866  S             20  4788224
rotee                29220      1    29219  S             20  4788224
rotee                29257      1    29256  S             20  4788224
rotee                29405      1    29404  S             20  4788224
rotee                29784      1    29783  S             20  4788224
oom.sh                5560   5246     5560  S             20  4427776
reflector.sh         15598      1    15598  S             20  3997696
droputil.sh          15600      1    15600  S             20  3997696
pvp.sh               24336      1    24335  S             20  3870720
pman.sh              29066  24336    24335  S             14  3805184
pman.sh              24643  24336    24335  S             14  3801088
pman.sh              27490  24336    24335  S             14  3801088
pman.sh              26696  24336    24335  S             14  3788800
pman.sh               9679  24336    24335  S             14  3784704
pman.sh               9812  24336    24335  S             14  3784704
pman.sh              24760  24336    24335  S             14  3784704
pman.sh              24917  24336    24335  S             14  3784704
pman.sh              25309  24336    24335  S             14  3784704
pman.sh              25617  24336    24335  S             14  3784704
pman.sh              26090  24336    24335  S             14  3784704
pman.sh              27718  24336    24335  S             14  3784704
pman.sh              28535  24336    24335  S             14  3784704
pman.sh              28948  24336    24335  S             14  3784704
pman.sh              29587  24336    24335  S             14  3784704
chasync.sh            5248      1     5248  S             20  3620864
```

```
lighttpd              11522   11521     10223  S            20  3543040
iptbl.sh               5252       1      5252  S            20  3477504
rollback_timer.        5226       1      5226  S            20  3014656
oom.sh                 5246       1      5246  S            20  2977792
wui-lighttpd-la       10223    9812     10223  S            20  2605056
wui-app-launch.       10210    9679     10210  S            20  2600960
mcp_chvrf.sh          10233   10210     10210  S            20  2596864
mcp_chvrf.sh          11521   10223     10223  S            20  2596864
auxinit.sh            15593       1     15593  S            20  2584576
mcp_chvrf.sh           5223       1      5223  S            20  2580480
mcp_chvrf.sh           5224       1      5224  S            20  2580480
libvirtd.sh            5254       1      5254  S            20  2576384
xinetd                 5231    5223      5223  S            20  2183168
xinetd                 5232    5224      5224  S            20  2183168
xinetd                15714       1     15714  S            20  2183168
xinetd                15716       1     15716  S            20  2183168
sleep                 30979   28469     28469  S            20  1925120
sleep                 31820    5560      5560  S            20  1925120
sleep                 32645   30092     30092  S            20  1925120
sntp                   5225       1      5225  S            20  1863680
init                      1       0         1  S            20  1859584
portmap                2654       1      2654  S            20  1806336
rpc.mountd            15751       1     15751  S            20  1789952
inotifywait            5459    5248      5459  S            20  1761280
inotifywait           16968   15598     16968  S            20  1761280
inotifywait           17050   15600     17050  S            20  1761280
inotifywait           24572   24336     24335  S            20  1761280
inotifywait            5462    5226      5462  S            20  1757184
inotifywait            5522    5252      5522  S            20  1757184
udevd                 13853       1     13853  S            16  1757184
inotifywait           32725   25251     32725  S            20  1757184
klogd                 24325       1     24325  S            20  1650688
kthreadd                  2       0         0  S            15  0
migration/0               3       2         0  S    4294967196  0
ksoftirqd/0               4       2         0  S            15  0
watchdog/0                5       2         0  S    4294967196  0
migration/1               6       2         0  S    4294967196  0
ksoftirqd/1               7       2         0  S            15  0
watchdog/1                8       2         0  S    4294967196  0
events/0                  9       2         0  S            15  0
events/1                 10       2         0  S            15  0
khelper                  11       2         0  S            15  0
netns                    14       2         0  S            15  0
kblockd/0                59       2         0  S            15  0
kblockd/1                60       2         0  S            15  0
kacpid                   61       2         0  S            15  0
kacpi_notify             62       2         0  S            15  0
cqueue                  144       2         0  S            15  0
ata/0                   148       2         0  S            15  0
ata/1                   149       2         0  S            15  0
ata_aux                 150       2         0  S            15  0
ksuspend_usbd           151       2         0  S            15  0
khubd                   156       2         0  S            15  0
kseriod                 159       2         0  S            15  0
pdflush                 210       2         0  S            20  0
pdflush                 211       2         0  S            20  0
kswapd0                 212       2         0  S            15  0
aio/0                   256       2         0  S            15  0
aio/1                   257       2         0  S            15  0
scsi_eh_0              1077       2         0  S            15  0
scsi_eh_1              1079       2         0  S            15  0
scsi_eh_2              1081       2         0  S            15  0
scsi_eh_3              1083       2         0  S            15  0
scsi_eh_4              1115       2         0  S            15  0
```

```
usb-storage             1116        2          0  S                 15   0
scsi_eh_5               1129        2          0  S                 15   0
usb-storage             1130        2          0  S                 15   0
scsi_eh_6               1133        2          0  S                 15   0
usb-storage             1134        2          0  S                 15   0
rpciod/0                2333        2          0  S                 15   0
rpciod/1                2336        2          0  S                 15   0
nfsiod                  2345        2          0  S                 15   0
loop0                   2424        2          0  S                  0   0
loop1                   2708        2          0  S                  0   0
loop2                   2745        2          0  S                  0   0
loop3                   2782        2          0  S                  0   0
loop4                   2819        2          0  S                  0   0
loop5                   2928        2          0  S                  0   0
loop6                   2965        2          0  S                  0   0
loop7                   3002        2          0  S                  0   0
loop8                   3075        2          0  S                  0   0
lockd                  15741        2          0  S                 15   0
nfsd                   15742        2          0  S                 15   0
nfsd                   15743        2          0  S                 15   0
nfsd                   15744        2          0  S                 15   0
nfsd                   15745        2          0  S                 15   0
nfsd                   15746        2          0  S                 15   0
nfsd                   15747        2          0  S                 15   0
nfsd                   15748        2          0  S                 15   0
nfsd                   15749        2          0  S                 15   0
lsmpi-refill           15852        2          0  S                 15   0
lsmpi-xmit             15853        2          0  S                 15   0
lsmpi-rx               15854        2          0  S                 15   0
ddr_err_monitor        16267        2          0  S                 15   0
mtdblockd              16292        2          0  S                 15   0
scansta                16315        2          0  S                 15   0
```

show platform software process memory

To display the memory statistics of a platform software process, use the **show platform software process memory** command in privileged EXEC mode or diagnostic mode.

show platform software process memory *host* {**name** *process-name* {**maps** | **smaps**} | **process-id** *process-id* {**maps** | **smaps**} | **all** [{**sorted** | **virtual** [{**sorted**}] | **rss** [{**sorted**}]}]}

Syntax Description

host	Process information. Possible *host* values are: • **0**—Cisco ASR 1000 Series SPA Interface Processor (SIP) slot 0 • **1**—Cisco ASR 1000 Series SIP slot 1 • **f0**—Cisco ASR 1000 Series Embedded Services Processor (ESP) slot 0 • **fp**—Cisco ASR 1000 Series ESP • **r0**—Cisco ASR 1000 Series Route Processor (RP) slot 0 • **rp**—Cisco ASR 1000 Series RP
name *process-name*	Displays the name of the specified process.
maps	Displays the memory maps of the specified process.
smaps	Displays the smaps of the specified process.
process-id *process-id*	Displays the ID of the specified process.
all	Lists all the processes.
sorted	Sorts the output from the highest size to the lowest size.
virtual	Displays the virtual memory footprint of all the processes.
rss	Displays the physical memory footprint of all the processes.

Command Modes

Privileged EXEC (#)

Diagnostic (diag)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.
Cisco IOS XE Release 3.9S	This command was modified. The **all**, **virtual**, and **rss** keywords were added.

Examples

The following is sample output of the **show platform software process memory** command on the host *r0* with the keywords **name** and **maps**:

```
Device# show platform software process memory r0 name smand maps

maps for process 29284:
address           perms offset   dev   inode      pathname
00100000-00103000 r-xp 00100000 00:00 0          [vdso]
0ebdb000-0ebe6000 r-xp 00000000 00:01 340        /lib/libnss_files.so.2
0ebe6000-0ebf5000 ---p 0000b000 00:01 340        /lib/libnss_files.so.2
0ebf5000-0ebf6000 r--p 0000a000 00:01 340        /lib/libnss_files.so.2
0ebf6000-0ebf7000 rwxp 0000b000 00:01 340        /lib/libnss_files.so.2
0ec07000-0ec0e000 r-xp 00000000 07:02 2310
/tmp/sw/mount/asr1000rp1-rpcontrol.2012-01-19_09.31_shpalani.pkg/usr/binos/lib/cdlapi.so
0ec0e000-0ec1d000 ---p 00007000 07:02 2310
/tmp/sw/mount/asr1000rp1-rpcontrol.2012-01-19_09.31_shpalani.pkg/usr/binos/lib/cdlapi.so
0ec1d000-0ec1e000 rwxp 00006000 07:02 2310
/tmp/sw/mount/asr1000rp1-rpcontrol.2012-01-19_09.31_shpalani.pkg/usr/binos/lib/cdlapi.so
0ec2e000-0ec30000 r-xp 00000000 07:02 4100
/tmp/sw/mount/asr1000rp1-rpcontrol.2012-01-19_09.31_shpalani.pkg/usr/binos/lib/trace.so
.
.
.
```

The following is sample output of the **show platform software process memory** command on the host *r0* with the keywords **process-id** and **maps**:

```
Device# show platform software process memory r0 process-id 1 maps

maps for process-id 1:
address           perms offset   dev   inode      pathname
00100000-00103000 r-xp 00100000 00:00 0          [vdso]
0fe2b000-0ff87000 r-xp 00000000 00:01 333        /lib/libc.so.6
0ff87000-0ff97000 ---p 0015c000 00:01 333        /lib/libc.so.6
0ff97000-0ff98000 r--p 0015c000 00:01 333        /lib/libc.so.6
0ff98000-0ff9c000 rwxp 0015d000 00:01 333        /lib/libc.so.6
0ff9c000-0ff9f000 rwxp 0ff9c000 00:00 0
0ffaf000-0ffb8000 r-xp 00000000 00:01 342        /lib/libcrypt.so.1
0ffb8000-0ffc7000 ---p 00009000 00:01 342        /lib/libcrypt.so.1
0ffc7000-0ffc8000 r--p 00008000 00:01 342        /lib/libcrypt.so.1
0ffc8000-0ffc9000 rwxp 00009000 00:01 342        /lib/libcrypt.so.1
0ffc9000-0fff0000 rwxp 0ffc9000 00:00 0
10000000-10008000 r-xp 00000000 00:01 149        /sbin/init
10017000-10018000 rwxp 00007000 00:01 149        /sbin/init
10018000-10039000 rwxp 10018000 00:00 0          [heap]
30000000-3001e000 r-xp 00000000 00:01 338        /lib/ld.so.1
3001e000-30021000 rw-p 3001e000 00:00 0
3002e000-3002f000 r--p 0001e000 00:01 338        /lib/ld.so.1
3002f000-30030000 rwxp 0001f000 00:01 338        /lib/ld.so.1
bfa9e000-bfab3000 rw-p bffe9000 00:00 0          [stack]
bfffe000-bffff000 r--p bfffe000 00:00 0
.
.
.
```

The following is sample output of the **show platform software process memory** command on the host *r0* with the keyword **all**:

```
Device# show platform software process memory r0 all

   Pid      VIRT       RSS       PSS      Heap    Shared   Private           Name
--------------------------------------------------------------------------------
     1      1820       516       119       132       404       112           init
  2195      1616       404        89       136       320        84          klogd
  2211      3892      2656      1623      1444      1056      1596         pvp.sh
```

```
  2258      4704      1592       410       132      1220       372         rotee
  2450      1724       500       106       136       404        96   inotifywait
  2519      3828      2560      1543      1380      1040      1516       pman.sh
  2596      3808      2544      1524      1360      1040      1500       pman.sh
  2634      4704      1592       417       132      1216       376         rotee
  2778      4704      1596       411       132      1220       376         rotee
  2868      3808      2544      1524      1360      1040      1500       pman.sh
.
.
.
```

The following is sample output of the **show platform software process memory** command on the host *r0* with the keywords **all** and **sorted**:

```
Device# show platform software process memory r0 all sorted

   Pid      VIRT       RSS       PSS      Heap    Shared   Private          Name
---------------------------------------------------------------------------------
  6559   5535152    644496    642116     29444      3768    640568  linux_iosd...
  8977    115232    108408    105527     99156      3312    105088         smand
  4708    758268     69688     67024      1744      3920     65768       fman_rp
 10074    197640     40700     38213       868      3564     37136          vman
  5081     24164     15116     11917      1192      4080     11036         imand
  8302    167472     13628     11125      1204      3592     10028   ptpd_mcp_rp
  3267     26928     12880      8721      2016      5920      6952         cmand
  4692     19136      7424      4100      2072      4424      3000           emd
  4252     15036      6456      3609      1072      3280      3176          hman
  7208     14940      5732      4455       684      1664      4068           psd
.
.
.
```

The following is sample output of the **show platform software process memory** command on the host *r0* with the keywords **all**, **virtual**, and **sorted**:

```
Device# show platform software process memory r0 all virtual sorted

Name               Pid   Virtual      Text   Shared Data   Private Data
----------------------------------------------------------------------
linux_iosd...     6559   5536756    287488         16888        5232380
fman_rp           4708    758264     64444         37796         656024
vman             10074    199244     15436         37924         145884
ptpd_mcp_rp       8302    169216     14308         10708         144200
smand             8977    116836      9908          3228         103700
cmand             3267     28684     20264          4256           4164
imand             5081     24160     10556         11164           2440
libvirtd         19860     23916      5020             0          18896
automount        23046     23472      2992             0          20480
emd               4692     19132     14052          1620           3460
pcscd             5576     18320      1520             0          16800
psd               7208     16544      9272          5284           1988
hman              4252     15032      9028          1620           4384
```

The following is sample output of the **show platform software process memory** command on the host *r0* with the keywords **all**, **rss**, and **sorted**:

```
Device# show platform software process memory r0 all rss sorted

Name               Pid       RSS      Text   Shared Data   Private Data
----------------------------------------------------------------------
linux_iosd...     6559    702284    172816          3128         526112
smand             8977    108780      5052           836         102884
```

```
fman_rp          4708     69140     27604           424          41112
vman            10074     40836      4752           332          35752
imand            5081     15084      3380          1256          10448
ptpd_mcp_rp      8302     13788      4584           312           8884
cmand            3267     13392      8040          1812           3532
emd              4692      7408      4284           148           2976
hman             4252      6476      3692           300           2484
psd              7208      5864      3848           408           1608
plogd            7170      5372      2632           384           2348
btrace_rot...    3090      3960      1044             0           2912
droputil.sh     22982      2844      1100             0           1740
```

The following table describes the significant fields shown in the display.

Table 225: show platform software process memory Field Descriptions

Field	Description
Address	Address space that the memory occupies in the process.
Perms	Set of permissions, such as: • **r**—Read • **w**—Write • **x**—Execute • **s**—Shared • **p**—Private
Offset	Offset into the file.
Dev	Number of the device.
Inode Number	Number of the inode on the device.
PathName	Location of the file.
Name	Name of the process.
PID	Process ID.
VIRT	Virtual memory size (in KB).
RSS	Resident Set Size (in KB).
PSS	Proportional Set Size (in KB).
Heap	Heap memory (in KB).
Shared	Memory and libraries shared with other processes (in KB).
Private	Memory that is exclusive to the specified process (in KB).

Related Commands

Command	Description
show platform software process list	Displays the list of processes running in a given slot.

show platform software ptp foreign-master

To display the PTP foreign-master information, use the show platform software ptp foreign-master command in privileged EXEC mode.

show platform software ptp [{**foreign-master**}] **domain** *domain-number*

Syntax Description

domain	Filters output by domain.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
IOS-XE 3.18	This command was introduced.

Usage Guidelines

Use this command to verify a PTP foreign-master information.

Examples

The following examples show the output generated by this command:

```
Router# show platform software ptp foreign-master domain 24

PTPd Foreign Master Information:

Current Master: SLA

Port: SLA
  Clock Identity: 0x74:A2:E6:FF:FE:5D:CE:3F
  Clock Stream Id: 0
  Priority1: 128
  Priority2: 128
  Local Priority: 128
  Clock Quality:
    Class: 6
    Accuracy: Within 100ns
    Offset (Log Variance): 0x4E5D
  Steps Removed: 1
  Not-Slave: FALSE
```

The table below describes significant fields shown in the display.

Table 226: show ptp clock dataset Field Descriptions

Field	Description
Current Master	Indicates the type of foreign master.
Port	Indicates the type of port.
Clock Identity	Unique identifier for the clock.
Priority1	Priority1 preference value of the PTP clock; the priority1 clock is considered first during clock selection.

Field	Description
Priority2	Priority2 preference value of the PTP clock; the priority2 clock is considered after all other clock sources during clock selection.
Local Priority	Indicates the PTP clock local priority.
Clock quality	Summarizes the quality of the grandmaster clock.
Class	Displays the time and frequency traceability of the grandmaster clock
Accuracy	Field applies only when the Best Master Clock algorithm is in use; indicates the expected accuracy of the master clock were the grandmaster clock.
Offset (log variance)	Offset between the local clock and an ideal reference clock.
Steps removed	Number of hops from the local clock to the grandmaster clock.
Not-Slave	Indicates whether the foreign master is a slave.

show platform software status control-processor

To display status information about the control processors, use the **showplatformsoftwarestatuscontrol-processor**command in privileged EXEC or diagnostic mode.

show platform software status control-processor [**brief**]

Syntax Description

brief	(Optional) Displays summary status information for the control processors.

Command Modes

Privileged EXEC (#) Diagnostic (diag)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 2.2	This command was modified. The **brief** keyword was added.

Usage Guidelines

Control processors consist of Embedded Services Processors (ESPs), Route Processors (RPs), and SPA Interface Processors (SIPs).

Use the **showplatformsoftwarestatuscontrol-processor** command to provide a quick view of the health of the system concerning memory and CPU usage on each processor.

The CPU usage output reflects the relative percentage of CPU usage during the latest two seconds instead of the cumulative percent usage over the entire uptime.

All control processors should show a status of Healthy. Other possible status values are Warning and Critical. Warning indicates that the router is operational but that the operating level should be reviewed. Critical implies that the router is near failure.

If you see a status of Warning or Critical, take the following actions:

- Reduce static and dynamic loads on the system by reducing the number of elements in the configuration or by limiting the capacity for dynamic services.
- Reduce the number of routes and adjacencies, limit the number of ACLs and other rules, reduce the number of VLANs, and so on.

Examples

The following example displays status information about the control processors:

```
Router# show platform software status control-processor
RP0: online, statistics updated 7 seconds ago
Load Average: healthy
  1-Min: 0.16, status: healthy, under 5.00
  5-Min: 0.16, status: healthy, under 5.00
  15-Min: 0.12, status: healthy, under 5.00
Memory (kb): healthy
  Total: 3733016
  Used: 1320804 (31%)
  Free: 2412212 (58%)
  Committed: 1889524 (45%), status: healthy, under 90%
```

```
ESP0: online, statistics updated 7 seconds ago
Load Average: healthy
  1-Min: 0.00, status: healthy, under 5.00
  5-Min: 0.00, status: healthy, under 5.00
  15-Min: 0.00, status: healthy, under 5.00
Memory (kb): healthy
  Total: 984996
  Used: 532492 (50%)
  Free: 452504 (43%)
  Committed: 1724096 (164%), status: healthy, under 300%
SIP0: online, statistics updated 10 seconds ago
Load Average: healthy
  1-Min: 0.00, status: healthy, under 5.00
  5-Min: 0.00, status: healthy, under 5.00
  15-Min: 0.00, status: healthy, under 5.00
Memory (kb): warning
  Total: 479884
  Used: 434476 (82%)
  Free: 45408 (8%)
  Committed: 202508 (38%), status: healthy, under 90%
SIP1: online, statistics updated 10 seconds ago
Load Average: healthy
  1-Min: 0.00, status: healthy, under 5.00
  5-Min: 0.00, status: healthy, under 5.00
  15-Min: 0.00, status: healthy, under 5.00
Memory (kb): warning
  Total: 479884
  Used: 430384 (82%)
  Free: 49500 (9%)
  Committed: 202512 (38%), status: healthy, under 90%
```

The following example displays summary status information about the control processors with **brief** keyword:

```
Router# show platform software status control-processor brief
Load Average
 Slot  Status  1-Min  5-Min 15-Min
  RP0 Healthy   0.25   0.30   0.44
  RP1 Healthy   0.31   0.19   0.12
 ESP0 Healthy   0.01   0.05   0.02
 ESP1 Healthy   0.03   0.05   0.01
 SIP1 Healthy   0.15   0.07   0.01
 SIP2 Healthy   0.03   0.03   0.00
Memory (kB)
 Slot  Status    Total     Used (Pct)     Free (Pct) Committed (Pct)
  RP0 Healthy  3722408  2514836 (60%)  1207572 (29%)   1891176 (45%)
  RP1 Healthy  3722408  2547488 (61%)  1174920 (28%)   1889976 (45%)
 ESP0 Healthy  2025468  1432088 (68%)   593380 (28%)   3136912 (149%)
 ESP1 Healthy  2025468  1377980 (65%)   647488 (30%)   3084412 (147%)
 SIP1 Healthy   480388   293084 (55%)   187304 (35%)    148532 (28%)
 SIP2 Healthy   480388   273992 (52%)   206396 (39%)     93188 (17%)
CPU Utilization
 Slot  CPU   User System   Nice   Idle    IRQ   SIRQ IOwait
  RP0    0  30.12   1.69   0.00  67.63   0.13   0.41   0.00
  RP1    0  21.98   1.13   0.00  76.54   0.04   0.12   0.16
 ESP0    0  13.37   4.77   0.00  81.58   0.07   0.19   0.00
 ESP1    0   5.76   3.56   0.00  90.58   0.03   0.05   0.00
 SIP1    0   3.79   0.13   0.00  96.04   0.00   0.02   0.00
 SIP2    0   3.50   0.12   0.00  96.34   0.00   0.02   0.00
```

The table below describes the significant fields shown in the display.

Table 227: show platform software status control-processor Field Descriptions

Field	Description
processor-name : online	Name of the online control processor to which the statistics that follow apply.
statistics updated x seconds ago	Time (in seconds) when the statistics were last updated.
Load Average:	Summary status indicator of the overall control processor load average. This value is derived from the “5-Min” load average.
1-Min: / status:	One-minute load average on the control processor and status indicator.
5-Min: / status:	Five-minute load average on the control processor and status indicator.
15-Min: / status:	Fifteen-minute load average on the control processor and status indicator.
Memory (kb):	Summary status indicator of the overall control processor memory usage. This value signals if any of the individual memory values below are in critical or warning status.
Total:	Total memory (in kilobytes) on the control processor.
Used: xxxxxxx (pp%)	Total used memory (in kilobytes) on the control processor and the percentage of used memory on the control processor.
Free: xxxxxxx (pp%)	Total free memory (in kilobytes) on the control processor and the percentage of free memory on the control processor.
Committed: xxxxxxx (pp%) / status:	Total committed memory (in kilobytes) on the control processor, percentage of committed memory on the control processor, and status indicator.
CPU Utilization:	Percentage of time that the CPU is busy.
CPU:	Allocated processor.
User:	Non-Linux kernel processes.
System:	Linux kernel process.
Nice:	Low priority processes.
Idle:	Percentage of time that the CPU was inactive.
IRQ:	Interrupts.
SIRQ:	System interrupts.
IOwait:	Percentage of time that the CPU was waiting for I/O.

Related Commands

Command	Description
show platform software process list	Displays a list of the processes running in a given slot.

show platform software punt-policer

To display the VLAN packets that are sent to the IOS on a Cisco ASR 1000 Router, use the **show platform software punt-policer** command in privileged EXEC mode.

show platform software punt-policer

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 3.2.0S	This command was introduced.
Cisco IOS XE 3.13.0S	This command was integrated into Cisco IOS XE Release 3.13.0S.

Example

The following is sample output of the **show platform software punt-policer** command:

```
Router# show platform software punt-policer

Punt                               Configured (pps)    Conform Packets     Dropped Packets
Cause      Description             Normal      High    Normal     High      Normal    High

-------------------------------------------------------------------------------------------
96       VLAN Auto Sense FSOL       2000       1000       0         0           0         0
```

The following table describes the significant fields shown in the display.

Table 228: show platform software punt-policer

Field	Description
Punt Cause	Indicates the punt cause number.
Description	Indicates the feature associated with a particular punt cause.
Configured (pps)	Indicates the number of packets the system handles for a particular VLAN. You can change the default maximum punt rate value 1000 by using the **platform punt-policer** *punt cause* command.
Conform Packets	Indicates the number of packets that conform to the rate limit.
Dropped Packets	Indicates the number of packets that are dropped.

show platform process slot

To monitor the software-running process in a given slot, use the **show platform software process slot**command in privileged EXEC or diagnostic mode.

show platform software process slot *slot* **monitor** [{**cycles** *cycles*}][{**interval** *delay*}][{**lines** *lines-of-output*}]

Syntax Description

slot	Specifies the Field Replace Unit (FRU) where the command is run.
slot	Slot information.
monitor	Monitors the running processes.
cycles	Checks the processes multiple times.
cycles	Number of times the command is run during a single invocation of the command. The range is from 1 to 4294967295. The default is 5.
interval	Sets delay interval after each command run.
delay	Delay between two successive runs of the command. The range is from 0 to 300. The default is 3.
lines	Sets the number of output lines that are displayed.
lines-of-output	Number of output lines displayed. The range is from 0 to 512. 0 displays all the lines. **Note** The number of lines is determined by the current terminal length.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1.0S	This command was introduced in a release earlier than Release 3.1.0S on Cisco ASR 1000 Series Routers.

Examples

The following is a sample output of the show platform software process slot command. Only 23 lines are displayed because the lines-of-output argument is set to 23:

```
Router# show platform software process slot 0 monitor cycles 3 interval 2 lines 23
top - 19:29:32 up 1 day,  4:46,  0 users,  load average: 0.10, 0.11, 0.09
Tasks:  78 total,   4 running,  74 sleeping,   0 stopped,   0 zombie
Cpu(s):  3.0%us,  2.9%sy,  0.0%ni, 93.9%id,  0.0%wa,  0.1%hi,  0.1%si,  0.0
Mem:    449752k total,   328940k used,   120812k free,     6436k buffers
Swap:        0k total,        0k used,        0k free,   155396k cached
  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 7223 root      20   0  124m  46m  23m R  2.0 10.5  11:13.01 mcpcc-lc-ms
 8135 root      20   0  123m  46m  25m R  2.0 10.6  35:59.75 mcpcc-lc-ms
```

```
    1 root      20   0  2156  644  556 S  0.0  0.1   0:02.05 init
    2 root      15  -5     0    0    0 S  0.0  0.0   0:00.04 kthreadd
    3 root      15  -5     0    0    0 S  0.0  0.0   0:00.00 ksoftirqd/0
    4 root      RT  -5     0    0    0 S  0.0  0.0   0:00.00 watchdog/0
    5 root      15  -5     0    0    0 S  0.0  0.0   0:00.04 events/0
    6 root      15  -5     0    0    0 S  0.0  0.0   0:00.10 khelper
    9 root      15  -5     0    0    0 S  0.0  0.0   0:00.00 netns
   55 root      15  -5     0    0    0 S  0.0  0.0   0:00.00 kblockd/0
   63 root      15  -5     0    0    0 S  0.0  0.0   0:00.00 ata/0
   64 root      15  -5     0    0    0 S  0.0  0.0   0:00.00 ata_aux
   70 root      15  -5     0    0    0 S  0.0  0.0   0:00.00 khubd
   73 root      15  -5     0    0    0 S  0.0  0.0   0:00.00 kseriod
  118 root      20   0     0    0    0 S  0.0  0.0   0:00.00 pdflush
  119 root      20   0     0    0    0 S  0.0  0.0   0:00.00 pdflush
top - 19:29:35 up 1 day,  4:46,  0 users,  load average: 0.41, 0.17, 0.11
 --More--
```

The table below describes the significant fields shown in the display.

Table 229: show platform software process slot Field Descriptions

Field	Description
%CPU	CPU Usage
%MEM	Memory Usage
COMMAND	Command name or command line
NI	Nice value
PID	Process ID
PR	Priority
RES	Resident memory size (in kb)
S	Process status
SHR	Shared memory size (in kb)
TIME+	Elapsed execution time
USER	User name
VIRT	Virtual memory size (in kb)

show platform software tech-support

To display system information or create a technical support information tar file for Cisco Technical Support, use the **show platform software tech-support**command in privileged EXEC or diagnostic mode.

show platform software tech-support [**file** {**bootflash:***filename***.tgz** | **fpd:***filename***.tgz** | **harddisk:***filename***.tgz** | **obfl:***filename***.tgz** | **stby-bootflash:***filename***.tgz** | **stby-harddisk:***filename***.tgz** | **stby-obfl:***filename***.tgz** | **stby-usb0:***filename***.tgz** | **stby-usb1:***filename***.tgz**}]

Syntax Description

file	(Optional) Creates a technical support information tar file for the specified destination file path.
bootflash: *filename* **.tgz**	Creates a technical support information tar file for the boot flash memory file system on the active RP.
fpd:*filename***.tgz**	Creates a technical support information tar file for the field-programmable device (FPD) image package on the active RP. The information displayed is for internal debugging puposes only.
harddisk:*filename* **.tgz**	Creates a technical support information tar file for the hard disk file system on the active RP.
obfl:*filename***.tgz**	Creates a technical support information tar file for the file system for Onboard Failure Logging (obfl) files. The information displayed is for internal debugging puposes only.
stby-bootflash: *filename* **.tgz**	Creates a technical support information tar file for the boot flash memory file system on the standby RP. The information displayed is for internal debugging puposes only.
stby-harddisk: *filename* **.tgz**	Creates a technical support information tar file for the hard disk file system on the standby RP. The information displayed is for internal debugging puposes only.
stby-obfl:*filename***.tgz**	Creates a technical support information tar file for the Onboard Failure Logging (obfl) files on the standby RP. The information displayed is for internal debugging puposes only.
stby-usb0:*filename***.tgz**	Creates a technical support information tar file for Universal Serial Bus (USB) memory. The information displayed is for internal debugging puposes only.
stby-usb1:*filename***.tgz**	Creates a technical support information tar file for Universal Serial Bus (USB) memory. The information displayed is for internal debugging puposes only.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Diagnostic (diag)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines

If the file keyword is specified, the specification of the bootflash: or harddisk: keyword and filename is required.

The show platform software tech-support command without a destination file path specification returns a large volume of information in a short period of time. You should save the output of the show platform software tech-support command in a log file to send to Cisco Technical Support for analysis.

Examples

The following example displays system information for Cisco Technical Support:

```
Router# show platform software tech-support
---- show version installed -----
Type: provisioning file, Version: unknown
  Provisioned on: RP0, Status: active
  File: packages.conf.super
  Modified: 2007-11-07 15:06:12.212303000 +0000
  SHA1 (header): d929d995d5ba2d3dedf67137c3e0e321b1727d7b
  SHA1 (calculated): d929d995d5ba2d3dedf67137c3e0e321b1727d7b
  SHA1 (external): a16881b6a7e3a5593b63bf211f72b8af9c534063
instance address        : 0X890DE9B4
    fast failover address   : 00000000
    cpp interface handle  0
    instance address        : 0X890DE9B8
    fast failover address   : 00000000
    cpp interface handle  0
    instance address        : 0X890DE9BC
    fast failover address   : 00000000
...
```

Note The show platform software tech-support command returns a large volume of information in a short period of time. The example above has been abbreviated for the purposes of this description.

The following example creates a technical support information tar file for the boot flash memory file system on the active RP:

```
Router# show platform software tech-support file bootflash:tech_support_output.tgz
Running tech support command set; please wait...
Creating file 'bootflash:target_support_output.tgz.tgz' ...
File 'bootflash:target_support_output.tgz.tgz' created successfully
```

The following example creates a technical support information tar file for the hard disk file system on the active RP:

```
Router# show platform software tech-support file harddisk:tech_support_output.tgz
Running tech support command set; please wait...
Creating file 'harddisk:tech_support_ouput.tgz.tgz' ...
File 'harddisk:tech_support_ouput.tgz.tgz' created successfully
```

show platform software vnic-if interface-mapping

To display the mapping between the virtual Network Interface Cards (vNICs) on the virtual machine (VM) and the network interfaces on the virtual router, use the **show platform software vnic-if interface-mapping** command in Privileged EXEC mode.

show platform software vnic-if interface-mapping

Command Modes

Privilged EXEC

Command History

Release	Modification
Cisco IOS XE Release 3.8S (Controlled Availability)	This command was introduced on the Cisco CSR 1000V Cloud Services Router.
Cisco IOS XE Release 3.10S	The command display fields were changed. The Short Name field was removed, and the vNIC Name field was changed to Driver Name.

Usage Guidelines

The GigabitEthernet0 interface configured on the Cisco CSR 1000V automatically maps to the vNIC designated as “eth0” on the VM.

All subsequent interfaces configured on the router are sequentially mapped to the corresponding vNIC interface on the VM. For example, the GigabitEthernet1 interface is mapped to the eth1 vNIC on the VM, and the GigabitEthernet2 interface is mapped to the eth2 vNIC.

The display for this command was changed in Cisco IOS XE 3.10S.

Examples

The following example displays the vNIC-to-interface mapping for Cisco IOS XE Release 3.9S and earlier:

```
Router# show platform software vnic-if interface-mapping
-------------------------------------------------------------------------
Interface Name        Short Name     vNIC Name           Mac Addr
-------------------------------------------------------------------------
GigabitEthernet0       Gi0        eth0 (vmxnet3)      000c.2946.3f4d
GigabitEthernet2       Gi2        eth2 (vmxnet3)      0050.5689.0034
GigabitEthernet1       Gi1        eth1 (vmxnet3)      0050.5689.000b
-------------------------------------------------------------------------
```

The following example displays the vNIC-to-interface mapping for Cisco IOS XE Release 3.10S and later:

```
csr1000v# show platform software vnic-if interface-mapping
--------------------------------------------------------------------------
Interface Name             Driver Name          Mac Addr
--------------------------------------------------------------------------
GigabitEthernet0            vmxnet3           000c.2946.3f4d
GigabitEthernet2            vmxnet3           0050.5689.0034
GigabitEthernet1            vmxnet3           0050.5689.000b
--------------------------------------------------------------------------
```

The following table describes the significant fields shown in the display.

Table 230: show platform software vnic-if interface-mapping Field Descriptions

Field	Description
Interface Name	The virtual router interface name.
Short Name	(Cisco IOS XE 3.9S and earlier) The virtual router short interface name.
vNIC Name	(Cisco IOS XE 3.9S and earlier) The virtual network interface on the VM that the virtual router interface is mapped to.
Driver Name	(Cisco IOS XE 3.10S and later) The vNIC driver type for the interface on the VM that the virtual router interface is mapped to.
Mac Addr	The MAC address on the VM's physical host that the virtual network interface (vNIC) is mapped to.

Related Commands

Command	Description
clear platform software vnic-if-nvtable	Clears the virtual router's persistent interface database on the original VM and updates the interface mapping to the hypervisor.

show platform time-source

To display the platform time-source details configured, use the **showplatformtime-source** command in the Privileged Exec mode .

show platform time-source

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)S	This command was introduced on the Cisco 7600 series routers.

Usage Guidelines

The**showplatformtime-source** command displays the platform time source configuration.

Examples

This example displays the show platform time source output:

```
Router#show platform time-source
 Time Source mode     : PTP
 PTP State            : Synchronized
 Master IP Address    : 200.1.1.2
 Slave IP Address     : 60.60.60.60
 UDP Source Port      : 51966
 UDP Destination Port : 320
 Control packets sent : 21
 Internal Vlan        : 1035
```

Related Commands

Command	Description
platform time-source	Initiates the Time of Day (ToD) synchroniztion on a line card.

show plim fpga

To display details gathered from the registers of the internal FPGA (Field Programmable Gate Array) located in the PLIM (Physical Layer Interface Module) section of the line card, use the **show plim fpga** command in privileged EXEC mode.

show plim fpga

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(33)S4	This command was introduced.

Usage Guidelines

This command helps you to troubleshoot datapath failures and get the datapath counters on Shiver FPGA.

The following information is available:

- Rx packet counter
- Tx packet counter
- Rx Error Counter
- Status and control register
- Door bell register status
- FPGA Binary image revision number
- Whether loop back is enabled
- Whether Ingress and Egress paths are enabled

Examples

The following example shows how to display the Shiver FPGA details:

```
Router# show plim fpga
***Shiver FPGA Stats***
FPGA Doorbell Register   : 0x00
FGPA binary image Revsion : 0xDD
FPGA Datapath Ctrl Reg   : 0x000B
 FPGA is Enabled in Eggress Direction
 FGPA is Enabled in Ingress Direction
 FPGA Eggress is Empty
======== Output from Tofab755 =======
FPGA Control and Status Register  : 0x028104dd
FPGA Rx Packet Count    : 0x000000cc
FPGA Tx Packet Count    : 0x000000cb
FPGA Rx Packet Error Count   : 0x0008ffff
```

The table below describes significant fields shown in the display.

Table 231: show plim fpga Field Descriptions

Field	Description
FPGA Doorbell Register	Line card's version of mailbox doorbell register.
FGPA binary image Revision	FPGA image version.
FPGA Datapath Ctrl Reg	Indicates whether the ingress and eggress paths are enabled or disabled.
Control and Status Register	A 32-bit read-write register that provides the MPC8260 processor with interrupt mask control, interrupt status, Rx Error status, and the FPGA revision ID.
Rx Packet Count	The number of packets received from the FREEDM-336 in the receive direction. This 32-bit count value saturates at 0xFFFF_FFFF. The counter is cleared when a write cycle is detected.
Tx Packet Count	The number of packets transmitted to the FREEDM-336. This 32-bit count value saturates at 0xFFFF_FFFF. The counter is cleared when a write cycle is detected.
Rx Packet Error Count	The number of packets with errors received from the FREEDM-336 in the receive direction. In this 32-bit counter, the 16 bit MSB (Most Significant Bit) indicates the errors that saturate after the value reaches FFFF. The value of LSB (Least Significant Bit) 16 bits will always be FFFF.

show policy-map interface

To display the statistics and the configurations of the input and output policies that are attached to an interface, use the **show policy-map interface** command in user EXEC or privileged EXEC mode.

ATM Shared Port Adapters

show policy-map interface *slot/subslot/port* **.**[*subinterface*]

Cisco CMTS Routers

show policy-map interface *interface-type slot/subslot/port*

Cisco 3660, 3845, 7200, 7400, 7500, Cisco ASR 903 Series Routers, and Cisco ASR 1000 Series Routers

show policy-map interface *type type-parameter* [**vc** [*vpi*][/]*vci*] [**dlci** *dlci*] [{**input** | **output**}] [**class** *class-name*]

Cisco 6500 Series Switches

show policy-map interface [{*interface-type interface-number* | **vlan** *vlan-id*}] [**detailed**] [{**input** | **output**} [**class** *class-name*]]

show policy-map interface [**port-channel** *channel-number* [**class** *class-name*]]

Cisco 7600 Series Routers

show policy-map interface [{*interface-type interface-number* | **null 0** | **vlan** *vlan-id*}] [{**input** | **output**}]

Syntax Description

slot	(CMTS and ATM shared port adapter only) Chassis slot number. See the appropriate hardware manual for slot information. For SIPs, see the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide.
/subslot	(CMTS and ATM shared port adapter only) Secondary slot number on an SPA interface processor (SIP) where a SPA is installed. See the platform-specific SPA hardware installation guide and the corresponding "Specifying the Interface Address on an SPA" topic in the platform-specific SPA software configuration guide for subslot information.
port	(CMTS and ATM shared port adapter only) Port or interface number. See the appropriate hardware manual for port information. For SPAs, see the corresponding "Specifying the Interface Address" topics in the platform-specific SPA software configuration guide.
.*subinterface*	(ATM shared port adapter only—Optional) Subinterface number. The number that precedes the period must match the number to which this subinterface belongs. The range is 1 to 4,294,967,293.
type	Type of interface or subinterface whose policy configuration is to be displayed.
type-parameter	Port, connector, interface card number, class-map name or other parameter associated with the interface or subinterface type.
vc	(Optional) For ATM interfaces only, shows the policy configuration for a specified PVC.

vpi /	(Optional) ATM network virtual path identifier (VPI) for this permanent virtual circuit (PVC). On the Cisco 7200 and 7500 series routers, this value ranges from 0 to 255. The *vpi* and *vci* arguments cannot both be set to 0; if one is 0, the other cannot be 0. The absence of both the forward slash (/) and a *vpi* value defaults the *vpi* value to 0. If this value is omitted, information for all virtual circuits (VCs) on the specified ATM interface or subinterface is displayed.
vci	(Optional) ATM network virtual channel identifier (VCI) for this PVC. This value ranges from 0 to 1 less than the maximum value set for this interface by the **atmvc-per-vp** command. Typically, the lower values 0 to 31 are reserved for specific traffic (F4 Operation, Administration, and Maintenance [OAM], switched virtual circuit [SVC] signaling, Integrated Local Management Interface [ILMI], and so on) and should not be used. The VCI is a 16-bit field in the header of the ATM cell. The VCI value is unique only on a single link, not throughout the ATM network, because it has local significance only. The *vpi* and *vci* arguments cannot both be set to 0; if one is 0, the other cannot be 0.
dlci	(Optional) Indicates a specific PVC for which policy configuration will be displayed.
dlci	(Optional) A specific data-link connection identifier (DLCI) number used on the interface. Policy configuration for the corresponding PVC will be displayed when a DLCI is specified.
input	(Optional) Indicates that the statistics for the attached input policy will be displayed.
output	(Optional) Indicates that the statistics for the attached output policy will be displayed.
class *class-name*	(Optional) Displays the QoS policy actions for the specified class.
interface-type	(Optional) Interface type; possible valid values are **atm**, **ethernet**, **fastethernet**, **ge-wan gigabitethernet**, **pos**, **pseudowire** and **tengigabitethernet**.
interface-number	(Optional) Module and port number; see the “Usage Guidelines” section for valid values.
vlan *vlan-id*	(Optional) Specifies the VLAN ID; valid values are from 1 to 4094.
detailed	(Optional) Displays additional statistics.
port-channel *channel-number*	(Optional) Displays the EtherChannel port-channel interface.
null 0	(Optional) Specifies the null interface; the only valid value is 0.

Command Default

This command displays the packet statistics of all classes that are configured for all service policies on the specified interface or subinterface or on a specific permanent virtual circuit (PVC) on the interface.

When used with the ATM shared port adapter, this command has no default behavior or values.

Command Modes

Privileged EXEC (#)

ATM Shared Port Adapter

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE.
12.0(7)S	This command was integrated into Cisco IOS Release 12.0(7)S.
12.0(28)S	This command was modified for the QoS: Percentage-Based Policing feature to include milliseconds when calculating the committed (conform) burst (bc) and excess (peak) burst (be) sizes.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(2)T	This command was modified to display information about the policy for all Frame Relay PVCs on the interface or, if a DLCI is specified, the policy for that specific PVC. This command was also modified to display the total number of packets marked by the quality of service (QoS) set action.
12.1(3)T	This command was modified to display per-class accounting statistics.
12.2(4)T	This command was modified for two-rate traffic policing and can display burst parameters and associated actions.
12.2(8)T	This command was modified for the Policer Enhancement—Multiple Actions feature and the WRED—Explicit Congestion Notification (ECN) feature. For the Policer Enhancement—Multiple Actions feature, the command was modified to display the multiple actions configured for packets conforming to, exceeding, or violating a specific rate. For the WRED—Explicit Congestion Notification (ECN) feature, the command displays ECN marking information.

Release	Modification
12.2(13)T	The following modifications were made: • This command was modified for the Percentage-Based Policing and Shaping feature. • This command was modified for the Class-Based RTP and TCP Header Compression feature. • This command was modified as part of the Modular QoS CLI (MQC) Unconditional Packet Discard feature. Traffic classes in policy maps can now be configured to discard packets belonging to a specified class. • This command was modified to display the Frame Relay DLCI number as a criterion for matching traffic inside a class map. • This command was modified to display Layer 3 packet length as a criterion for matching traffic inside a class map. • This command was modified for the Enhanced Packet Marking feature. A mapping table (table map) can now be used to convert and propagate packet-marking values.
12.2(14)SX	This command was modified. Support for this command was introduced on Cisco 7600 series routers.
12.2(15)T	This command was modified to display Frame Relay voice-adaptive traffic-shaping information.
12.2(17d)SXB	This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB.
12.3(14)T	This command was modified to display bandwidth estimation parameters.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE. This command was modified to display aggregate WRED statistics for the ATM shared port adapter. Note that changes were made to the syntax, defaults, and command modes. These changes are labelled “ATM Shared Port Adapter.”
12.4(4)T	This command was modified. The **typeaccess-control** keywords were added to support flexible packet matching.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB, and the following modifications were made: • This command was modified to display either legacy (undistributed processing) QoS or hierarchical queueing framework (HQF) parameters on Frame Relay interfaces or PVCs. • This command was modified to display information about Layer 2 Tunnel Protocol Version 3 (L2TPv3) tunnel marking.

Release	Modification
12.2(31)SB2	The following modifications were made: • This command was enhanced to display statistical information for each level of priority service configured and information about bandwidth-remaining ratios, and this command was implemented on the Cisco 10000 series router for the PRE3. • This command was modified to display statistics for matching packets on the basis of VLAN identification numbers. As of Cisco IOS Release 12.2(31)SB2, matching packets on the basis of VLAN identification numbers is supported on Cisco 10000 series routers only.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.4(15)T2	This command was modified to display information about Generic Routing Encapsulation (GRE) tunnel marking. **Note** As of this release, GRE-tunnel marking is supported on the Cisco MGX Route Processor Module (RPM-XF) platform *only* .
12.2(33)SB	This command was modified to display information about GRE-tunnel marking, and support for the Cisco 7300 series router was added.
Cisco IOS XE 2.1	This command was integrated into Cisco IOS XE Release 2.1 and was implemented on the Cisco ASR 1000 series router.
12.4(20)T	This command was modified. Support was added for hierarchical queueing framework (HQF) using the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC).
12.2(33)SXI	This command was implemented on the Catalyst 6500 series switch and modified to display the strict level in the priority feature and the counts per level.
12.2(33)SRE	This command was modified to automatically round off the bc and be values, in the MQC police policy map, to the interface's MTU size.
Cisco IOS XE Release 2.6	The command output was modified to display information about subscriber QoS statistics.
12.2(54)SG	This command was modified to display only the applicable count of policer statistics.
12.2(33)SCF	This command was integrated into Cisco IOS Release 12.2(33)SCF.
Cisco IOS XE Release 3.7S	This command was implemented on Cisco ASR 903 Series Routers.
Cisco IOS XE Release 3.8S	This command was modified. The *pseudowire* interface type was added.
Cisco IOS XE Release 3.8S	This command was modified. The *pseudowire* interface type was added on Cisco 1000 Series Routers.

Release	Modification
Cisco IOS Release 15.3(1)S	This command was modified. The *pseudowire* interface type was added.

Usage Guidelines

Cisco 3660, 3845, 7200, 7400, 7500, Cisco ASR 903 Series Routers, and Cisco ASR 1000 Series Routers

The **show policy-map interface** command displays the packet statistics for classes on the specified interface or the specified PVC only if a service policy has been attached to the interface or the PVC.

The counters displayed after the **show policy-map interface** command is entered are updated only if congestion is present on the interface.

The **show policy-map interface** command displays policy information about Frame Relay PVCs only if Frame Relay Traffic Shaping (FRTS) is enabled on the interface.

The **show policy-map interface** command displays ECN marking information only if ECN is enabled on the interface.

To determine if shaping is active with HQF, check the queue depth field of the "(queue depth/total drops/no-buffer drops)" line in the **show policy-map interface** command output.

In HQF images for Cisco IOS Releases 12.4(20)T and later, the packets delayed and the bytes delayed counters were removed for traffic shaping classes.

Cisco 7600 Series Routers and Catalyst 6500 Series Switches

The pos, atm, and ge-wan interfaces are not supported on Cisco 7600 series routers or Catalyst 6500 series switches that are configured with a Supervisor Engine 720

Cisco 7600 series routers and Catalyst 6500 series switches that are configured with a Supervisor Engine 2 display packet counters.

Cisco 7600 series routers and Catalyst 6500 series switches that are configured with a Supervisor Engine 720 display byte counters.

The output does not display policed-counter information; 0 is displayed in its place (for example, 0 packets, 0 bytes). To display dropped and forwarded policed-counter information, enter the **show mls qos** command.

On the Cisco 7600 series router, for OSM WAN interfaces only, if you configure policing within a policy map, the hardware counters are displayed and the class-default counters are not displayed. If you do not configure policing within a policy map, the class-default counters are displayed.

On the Catalyst 6500 series switch, the **show policy-map interface** command displays the strict level in the priority feature and the counts per level.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

HQF

When you configure HQF, the **show policy-map interface** command displays additional fields that include the differentiated services code point (DSCP) value, WRED statistics in bytes, transmitted packets by WRED, and a counter that displays packets output/bytes output in each class.

Examples

This section provides sample output from typical **show policy-map interface** commands. Depending upon the interface or platform in use and the options enabled, the output you see may vary slightly from the ones shown below.

Weighted Fair Queueing (WFQ) on Serial Interface: Example

The following sample output of the **show policy-map interface** command displays the statistics for the serial 3/1 interface, to which a service policy called mypolicy (configured as shown below) is attached. Weighted fair queueing (WFQ) has been enabled on this interface. See the table below for an explanation of the significant fields that commonly appear in the command output.

```
policy-map mypolicy
 class voice
  priority 128
 class gold
  bandwidth 100
 class silver
  bandwidth 80
  random-detect
Router# show policy-map interface serial3/1 output

 Serial3/1
  Service-policy output: mypolicy
    Class-map: voice (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 5
      Weighted Fair Queueing
        Strict Priority
        Output Queue: Conversation 264
        Bandwidth 128 (kbps) Burst 3200 (Bytes)
        (pkts matched/bytes matched) 0/0
        (total drops/bytes drops) 0/0
    Class-map: gold (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 2
      Weighted Fair Queueing
        Output Queue: Conversation 265
        Bandwidth 100 (kbps) Max Threshold 64 (packets)
        (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0
    Class-map: silver (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 1
      Weighted Fair Queueing
        Output Queue: Conversation 266
        Bandwidth 80 (kbps)
        (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0
         exponential weight: 9
         mean queue depth: 0
class     Transmitted       Random drop      Tail drop    Minimum Maximum  Mark
          pkts/bytes        pkts/bytes       pkts/bytes    thresh  thresh  prob
0             0/0               0/0              0/0           20      40  1/10
1             0/0               0/0              0/0           22      40  1/10
2             0/0               0/0              0/0           24      40  1/10
3             0/0               0/0              0/0           26      40  1/10
```

```
4             0/0               0/0               0/0             28      40  1/10
5             0/0               0/0               0/0             30      40  1/10
6             0/0               0/0               0/0             32      40  1/10
7             0/0               0/0               0/0             34      40  1/10
rsvp          0/0               0/0               0/0             36      40  1/10
Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

Traffic Shaping on Serial Interface: Example

The following sample output from the **show policy-map interface** command displays the statistics for the serial 3/2 interface, to which a service policy called p1 (configured as shown below) is attached. Traffic shaping has been enabled on this interface. See the table below for an explanation of the significant fields that commonly appear in the command output.

Note In HQF images for Cisco IOS Releases 12.4(20)T and later, the packets delayed and bytes delayed counters were removed for traffic shaping classes.

```
policy-map p1
 class c1
  shape average 320000
Router# show policy-map interface serial3/2 output

 Serial3/2
  Service-policy output: p1
    Class-map: c1 (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 0
      Traffic Shaping
        Target    Byte   Sustain   Excess    Interval  Increment Adapt
        Rate      Limit  bits/int  bits/int  (ms)      (bytes)   Active
        320000    2000   8000      8000      25        1000      -
        Queue     Packets   Bytes     Packets   Bytes     Shaping
        Depth                         Delayed   Delayed   Active
        0         0         0         0         0         no
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

The table below describes significant fields commonly shown in the displays. The fields in the table are grouped according to the relevant QoS feature. A number in parentheses may appear next to the service-policy output name, class-map name, and match criteria information. The number is for Cisco internal use only and can be disregarded.

Table 232: show policy-map interface Field Descriptions

Field	Description
Fields Associated with Classes or Service Policies	

Field	Description
Service-policy output	Name of the output service policy applied to the specified interface or VC.
Class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets and bytes	Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
offered rate	Rate, in kbps, of packets coming in to the class. **Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only.
drop rate	Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate.

Field	Description
Note In distributed architecture platforms (such as the Cisco 7500 series platform), the value of the transfer rate, calculated as the difference between the offered rate and the drop rate counters, can sporadically deviate from the average by up to 20 percent or more. This can occur while no corresponding burst is registered by independent traffic analyser equipment.	
Match	Match criteria specified for the class of traffic. Choices include criteria such as IP precedence, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental (EXP) value, access groups, and QoS groups. For more information about the variety of match criteria that are available, see the "Classifying Network Traffic" module in the *Cisco IOS Quality of Service Solutions Configuration Guide* .
Fields Associated with Queueing (if Enabled)	
Output Queue	The weighted fair queueing (WFQ) conversation to which this class of traffic is allocated.
Bandwidth	Bandwidth, in either kbps or percentage, configured for this class and the burst size.
pkts matched/bytes matched	Number of packets (also shown in bytes) matching this class that were placed in the queue. This number reflects the total number of matching packets queued at any time. Packets matching this class are queued only when congestion exists. If packets match the class but are never queued because the network was not congested, those packets are not included in this total. However, if process switching is in use, the number of packets is always incremented even if the network is not congested.
depth/total drops/no-buffer drops	Number of packets discarded for this class. No-buffer indicates that no memory buffer exists to service the packet.

Field	Description
Fields Associated with Weighted Random Early Detection (WRED) (if Enabled)	
exponential weight	Exponent used in the average queue size calculation for a WRED parameter group.
mean queue depth	Average queue depth based on the actual queue depth on the interface and the exponential weighting constant. It is a fluctuating average. The minimum and maximum thresholds are compared against this value to determine drop decisions.
class	IP precedence level.
Transmitted pkts/bytes	Number of packets (also shown in bytes) passed through WRED and not dropped by WRED. **Note** If there is insufficient memory in the buffer to accommodate the packet, the packet can be dropped *after* the packet passes through WRED. Packets dropped because of insufficient memory in the buffer (sometimes referred to as “no-buffer drops”) are not taken into account by the WRED packet counter.
Random drop pkts/bytes	Number of packets (also shown in bytes) randomly dropped when the mean queue depth is between the minimum threshold value and the maximum threshold value for the specified IP precedence level.
Tail drop pkts/bytes	Number of packets dropped when the mean queue depth is greater than the maximum threshold value for the specified IP precedence level.
Minimum thresh	Minimum threshold. Minimum WRED threshold in number of packets.
Maximum thresh	Maximum threshold. Maximum WRED threshold in number of packets.
Mark prob	Mark probability. Fraction of packets dropped when the average queue depth is at the maximum threshold.
Fields Associated with Traffic Shaping (if Enabled)	
Target Rate	Rate used for shaping traffic.
Byte Limit	Maximum number of bytes that can be transmitted per interval. Calculated as follows: ((Bc+Be) /8) x 1
Sustain bits/int	Committed burst (Bc) rate.
Excess bits/int	Excess burst (Be) rate.
Interval (ms)	Time interval value in milliseconds (ms).

Field	Description
Increment (bytes)	Number of credits (in bytes) received in the token bucket of the traffic shaper during each time interval.
Queue Depth	Current queue depth of the traffic shaper.
Packets	Total number of packets that have entered the traffic shaper system.
Bytes	Total number of bytes that have entered the traffic shaper system.
Packets Delayed	Total number of packets delayed in the queue of the traffic shaper before being transmitted.
Bytes Delayed	Total number of bytes delayed in the queue of the traffic shaper before being transmitted.
Shaping Active	Indicates whether the traffic shaper is active. For example, if a traffic shaper is active, and the traffic being sent exceeds the traffic shaping rate, a "yes" appears in this field.

Precedence-Based Aggregate WRED on ATM Shared Port Adapter: Example

The following sample output of the **show policy-map interface** command displays the statistics for the ATM shared port adapter interface 4/1/0.10, to which a service policy called prec-aggr-wred (configured as shown below) is attached. Because aggregate WRED has been enabled on this interface, the classthrough Mark Prob statistics are aggregated by subclasses. See the table below for an explanation of the significant fields that commonly appear in the command output.

```
Router(config)# policy-map prec-aggr-wred
Router(config-pmap)# class class-default
Router(config-pmap-c)# random-detect aggregate
Router(config-pmap-c)# random-detect precedence values 0 1 2 3 minimum thresh 10
maximum-thresh 100 mark-prob 10
Router(config-pmap-c)# random-detect precedence values 4 5 minimum-thresh 40 maximum-thresh
 400 mark-prob 10
Router(config-pmap-c)# random-detect precedence values 6 minimum-thresh 60 maximum-thresh
600 mark-prob 10
Router(config-pmap-c)# random-detect precedence values 7 minimum-thresh 70 maximum-thresh
700 mark-prob 10
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface ATM4/1/0.10 point-to-point
Router(config-if)# ip address 10.0.0.2 255.255.255.0
Router(config-if)# pvc 10/110
Router(config-if)# service-policy output prec-aggr-wred
```

```
Router# show policy-map interface atm4/1/0.10

 ATM4/1/0.10: VC 10/110 -
  Service-policy output: prec-aggr-wred
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

```
        Exp-weight-constant: 9 (1/512)
        Mean queue depth: 0
        class       Transmitted     Random drop      Tail drop     Minimum   Maximum  Mark
 pkts/bytes pkts/bytes pkts/bytes thresh thresh prob

        0  1  2  3       0/0              0/0              0/0           10     100  1/10
        4  5             0/0              0/0              0/0           40     400  1/10
        6                0/0              0/0              0/0           60     600  1/10
        7                0/0              0/0              0/0           70     700  1/10
```

DSCP-Based Aggregate WRED on ATM Shared Port Adapter: Example

The following sample output of the **show policy-map interface** command displays the statistics for the ATM shared port adapter interface 4/1/0.11, to which a service policy called dscp-aggr-wred (configured as shown below) is attached. Because aggregate WRED has been enabled on this interface, the class through Mark Prob statistics are aggregated by subclasses. See the table below for an explanation of the significant fields that commonly appear in the command output.

```
Router(config)# policy-map dscp-aggr-wred
Router(config-pmap)# class class-default
Router(config-pmap-c)# random-detect dscp-based aggregate minimum-thresh 1 maximum-thresh
10 mark-prob 10
Router(config-pmap-c)# random-detect dscp values 0 1 2 3 4 5 6 7 minimum-thresh 10
maximum-thresh 20 mark-prob 10
Router(config-pmap-c)# random-detect dscp values 8 9 10 11 minimum-thresh 10 maximum-thresh
 40 mark-prob 10
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface ATM4/1/0.11 point-to-point
Router(config-subif)# ip address 10.0.0.2 255.255.255.0
Router(config-subif)# pvc 11/101
Router(config-subif)# service-policy output dscp-aggr-wred
Router# show policy-map interface atm4/1/0.11

 ATM4/1/0.11: VC 11/101 -
  Service-policy output: dscp-aggr-wred
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
        Exp-weight-constant: 0 (1/1)
        Mean queue depth: 0
        class       Transmitted     Random drop      Tail drop     Minimum   Maximum  Mark
                  pkts/bytes pkts/bytes pkts/bytes thresh thresh prob
        default          0/0              0/0              0/0            1      10  1/10
        0  1  2  3
        4  5  6  7       0/0              0/0              0/0           10      20  1/10
        8  9  10 11      0/0              0/0              0/0           10      40  1/10
```

The table below describes the significant fields shown in the display when aggregate WRED is configured for an ATM shared port adapter.

Table 233: show policy-map interface Field Descriptions—Configured for Aggregate WRED on ATM Shared Port Adapter

Field	Description
exponential weight	Exponent used in the average queue size calculation for a Weighted Random Early Detection (WRED) parameter group.

Field	Description
mean queue depth	Average queue depth based on the actual queue depth on the interface and the exponential weighting constant. It is a fluctuating average. The minimum and maximum thresholds are compared against this value to determine drop decisions.
Note When Aggregate Weighted Random Early Detection (WRED) is enabled, the following WRED statistics will be aggregated based on their subclass (either their IP precedence or differentiated services code point (DSCP) value).	
class	IP precedence level or differentiated services code point (DSCP) value.
Transmitted pkts/bytes	Number of packets (also shown in bytes) passed through WRED and not dropped by WRED. **Note** If there is insufficient memory in the buffer to accommodate the packet, the packet can be dropped *after* the packet passes through WRED. Packets dropped because of insufficient memory in the buffer (sometimes referred to as “no-buffer drops”) are not taken into account by the WRED packet counter.
Random drop pkts/bytes	Number of packets (also shown in bytes) randomly dropped when the mean queue depth is between the minimum threshold value and the maximum threshold value for the specified IP precedence level or DSCP value.
Tail drop pkts/bytes	Number of packets dropped when the mean queue depth is greater than the maximum threshold value for the specified IP precedence level or DSCP value.
Minimum thresh	Minimum threshold. Minimum WRED threshold in number of packets.
Maximum thresh	Maximum threshold. Maximum WRED threshold in number of packets.
Mark prob	Mark probability. Fraction of packets dropped when the average queue depth is at the maximum threshold.

Frame Relay Voice-Adaptive Traffic-Shaping: Example

The following sample output shows that Frame Relay voice-adaptive traffic shaping is currently active and has 29 seconds left on the deactivation timer. With traffic shaping active and the deactivation time set, this means that the current sending rate on DLCI 201 is minCIR, but if no voice packets are detected for 29 seconds, the sending rate will increase to CIR.

Note In HQF images for Cisco IOS Releases 12.4(20)T and later, the packets delayed and bytes delayed counters were removed for traffic shaping classes.

```
Router# show policy interface Serial3/1.1

 Serial3/1.1:DLCI 201 -
  Service-policy output:MQC-SHAPE-LLQ1

    Class-map:class-default (match-any)
      1434 packets, 148751 bytes
      30 second offered rate 14000 bps, drop rate 0 bps
      Match:any
      Traffic Shaping
           Target/Average   Byte   Sustain   Excess    Interval  Increment
             Rate           Limit  bits/int  bits/int  (ms)      (bytes)
            63000/63000     1890   7560      7560      120       945

        Adapt  Queue     Packets   Bytes     Packets   Bytes     Shaping
        Active Depth                         Delayed   Delayed   Active
        BECN   0         1434      162991    26        2704      yes
        Voice Adaptive Shaping active, time left 29 secs
```

The table below describes the significant fields shown in the display. Significant fields that are not described in the table below are described in the table above (for "show policy-map interface Field Descriptions").

Table 234: show policy-map interface Field Descriptions—Configured for Frame Relay Voice-Adaptive Traffic Shaping

Field	Description
Voice Adaptive Shaping active/inactive	Indicates whether Frame Relay voice-adaptive traffic shaping is active or inactive.
time left	Number of seconds left on the Frame Relay voice-adaptive traffic shaping deactivation timer.

Two-Rate Traffic Policing: Example

The following is sample output from the **show policy-map interface** command when two-rate traffic policing has been configured. In the example below, 1.25 Mbps of traffic is sent ("offered") to a policer class.

```
Router# show policy-map interface serial3/0
```

```
Serial3/0
 Service-policy output: policy1
  Class-map: police (match all)
   148803 packets, 36605538 bytes
   30 second offered rate 1249000 bps, drop rate 249000 bps
   Match: access-group 101
   police:
    cir 500000 bps, conform-burst 10000, pir 1000000, peak-burst 100000
    conformed 59538 packets, 14646348 bytes; action: transmit
    exceeded 59538 packets, 14646348 bytes; action: set-prec-transmit 2
    violated 29731 packets, 7313826 bytes; action: drop
    conformed 499000 bps, exceed 500000 bps violate 249000 bps
  Class-map: class-default (match-any)
   19 packets, 1990 bytes
   30 seconds offered rate 0 bps, drop rate 0 bps
   Match: any
```

The two-rate traffic policer marks 500 kbps of traffic as conforming, 500 kbps of traffic as exceeding, and 250 kbps of traffic as violating the specified rate. Packets marked as conforming will be sent as is, and packets marked as exceeding will be marked with IP Precedence 2 and then sent. Packets marked as violating the specified rate are dropped.

The table below describes the significant fields shown in the display.

Table 235: show policy-map interface Field Descriptions—Configured for Two-Rate Traffic Policing

Field	Description
police	Indicates that the **police** command has been configured to enable traffic policing. Also, displays the specified CIR, conform burst size, peak information rate (PIR), and peak burst size used for marking packets.
conformed	Displays the action to be taken on packets conforming to a specified rate. Displays the number of packets and bytes on which the action was taken.
exceeded	Displays the action to be taken on packets exceeding a specified rate. Displays the number of packets and bytes on which the action was taken.
violated	Displays the action to be taken on packets violating a specified rate. Displays the number of packets and bytes on which the action was taken.

Multiple Traffic Policing Actions: Example

The following is sample output from the **show policy-map** command when the Policer Enhancement—Multiple Actions feature has been configured. The sample output from the **show policy-map interface** command displays the statistics for the serial 3/2 interface, to which a service policy called “police” (configured as shown below) is attached.

```
policy-map police
 class class-default
  police cir 1000000 pir 2000000
   conform-action transmit
   exceed-action set-prec-transmit 4
   exceed-action set-frde-transmit
   violate-action set-prec-transmit 2
   violate-action set-frde-transmit
```

```
Router# show policy-map interface serial3/2

Serial3/2: DLCI 100 -
Service-policy output: police
    Class-map: class-default (match-any)
      172984 packets, 42553700 bytes
      5 minute offered rate 960000 bps, drop rate 277000 bps
      Match: any
     police:
         cir 1000000 bps, bc 31250 bytes, pir 2000000 bps, be 31250 bytes
       conformed 59679 packets, 14680670 bytes; actions:
         transmit
exceeded 59549 packets, 14649054 bytes; actions:
         set-prec-transmit 4
         set-frde-transmit
       violated 53758 packets, 13224468 bytes; actions:
         set-prec-transmit 2
         set-frde-transmit
       conformed 340000 bps, exceed 341000 bps, violate 314000 bps
```

The sample output from **show policy-map interface** command shows the following:

- 59679 packets were marked as conforming packets (that is, packets conforming to the CIR) and were transmitted unaltered.
- 59549 packets were marked as exceeding packets (that is, packets exceeding the CIR but not exceeding the PIR). Therefore, the IP Precedence value of these packets was changed to an IP Precedence level of 4, the discard eligibility (DE) bit was set to 1, and the packets were transmitted with these changes.
- 53758 packets were marked as violating packets (that is, exceeding the PIR). Therefore, the IP Precedence value of these packets was changed to an IP Precedence level of 2, the DE bit was set to 1, and the packets were transmitted with these changes.

Note Actions are specified by using the *action* argument of the **police** command. For more information about the available actions, see the **police** command reference page.

The table below describes the significant fields shown in the display.

Table 236: show policy-map interface Field Descriptions—Configured for Multiple Traffic Policing Actions

Field	Description
police	Indicates that the **police** command has been configured to enable traffic policing. Also, displays the specified CIR, conform burst size (BC), PIR, and peak burst size (BE) used for marking packets.
conformed, packets, bytes, actions	Displays the number of packets (also shown in bytes) marked as conforming to a specified rate and the actions taken on the packet. If there are multiple actions, each action is listed separately.
exceeded, packets, bytes, actions	Displays the number of packets (also shown in bytes) marked as exceeding a specified rate and the actions taken on the packet. If there are multiple actions, each action is listed separately.

Field	Description
violated, packets, bytes, actions	Displays the number of packets (also shown in bytes) marked as violating a specified rate and the actions taken on the packet. If there are multiple actions, each action is listed separately.

Explicit Congestion Notification: Example

The following is sample output from the **show policy-map interface** command when the WRED — Explicit Congestion Notification (ECN) feature has been configured. The words "explicit congestion notification" included in the output indicate that ECN has been enabled.

```
Router# show policy-map interface Serial4/1

 Serial4/1
  Service-policy output:policy_ecn
        Class-map:prec1 (match-all)
          1000 packets, 125000 bytes
          30 second offered rate 14000 bps, drop rate 5000 bps
          Match:ip precedence 1
          Weighted Fair Queueing
            Output Queue:Conversation 42
            Bandwidth 20 (%)
            Bandwidth 100 (kbps)
            (pkts matched/bytes matched) 989/123625
        (depth/total drops/no-buffer drops) 0/455/0
             exponential weight:9
             explicit congestion notification
             mean queue depth:0
     class   Transmitted  Random drop  Tail drop   Minimum     Maximum     Mark
             pkts/bytes   pkts/bytes    pkts/bytes threshold   threshold   probability
       0       0/0          0/0          0/0          20          40        1/10
       1     545/68125      0/0          0/0          22          40        1/10
       2       0/0          0/0          0/0          24          40        1/10
       3       0/0          0/0          0/0          26          40        1/10
       4       0/0          0/0          0/0          28          40        1/10
       5       0/0          0/0          0/0          30          40        1/10
       6       0/0          0/0          0/0          32          40        1/10
       7       0/0          0/0          0/0          34          40        1/10
     rsvp      0/0          0/0          0/0          36          40        1/10
     class   ECN Mark
            pkts/bytes
       0     0/0
       1    43/5375
       2     0/0
       3     0/0
       4     0/0
       5     0/0
       6     0/0
       7     0/0
     rsvp    0/0
```

The table below describes the significant fields shown in the display.

Table 237: show policy-map interface Field Descriptions—Configured for ECN

Field	Description
explicit congestion notification	Indication that Explicit Congestion Notification is enabled.
mean queue depth	Average queue depth based on the actual queue depth on the interface and the exponential weighting constant. It is a moving average. The minimum and maximum thresholds are compared against this value to determine drop decisions.
class	IP precedence value.
Transmitted pkts/bytes	Number of packets (also shown in bytes) passed through WRED and not dropped by WRED. **Note** If there is insufficient memory in the buffer to accommodate the packet, the packet can be dropped *after* the packet passes through WRED. Packets dropped because of insufficient memory in the buffer (sometimes referred to as “no-buffer drops”) are not taken into account by the WRED packet counter.
Random drop pkts/bytes	Number of packets (also shown in bytes) randomly dropped when the mean queue depth is between the minimum threshold value and the maximum threshold value for the specified IP precedence value.
Tail drop pkts/bytes	Number of packets dropped when the mean queue depth is greater than the maximum threshold value for the specified IP precedence value.
Minimum threshold	Minimum WRED threshold in number of packets.
Maximum threshold	Maximum WRED threshold in number of packets.
Mark probability	Fraction of packets dropped when the average queue depth is at the maximum threshold.
ECN Mark pkts/bytes	Number of packets (also shown in bytes) marked by ECN.

Class-Based RTP and TCP Header Compression: Example

The following sample output from the **show policy-map interface** command shows the RTP header compression has been configured for a class called “prec2” in the policy map called “p1”.

The **show policy-map interface** command output displays the type of header compression configured (RTP), the interface to which the policy map called “p1” is attached (Serial 4/1), the total number of packets, the number of packets compressed, the number of packets saved, the number of packets sent, and the rate at which the packets were compressed (in bits per second (bps)).

In this example, User Datagram Protocol (UDP)/RTP header compressions have been configured, and the compression statistics are included at the end of the display.

```
Router# show policy-map interface Serial4/1
```

```
Serial4/1
Service-policy output:p1
    Class-map:class-default (match-any)
      1005 packets, 64320 bytes
      30 second offered rate 16000 bps, drop rate 0 bps
      Match:any
compress:
          header ip rtp
          UDP/RTP Compression:
          Sent:1000 total, 999 compressed,
                41957 bytes saved, 17983 bytes sent
                3.33 efficiency improvement factor
                99% hit ratio, five minute miss rate 0 misses/sec, 0 max
                 rate 5000 bps
```

The table below describes the significant fields shown in the display.

Table 238: show policy-map interface Field Descriptions—Configured for Class-Based RTP and TCP Header Compression

Field	Description
Service-policy output	Name of the output service policy applied to the specified interface or VC.
Class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets, bytes	Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
offered rate	Rate, in kbps, of packets coming in to the class. **Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only.
UDP/RTP Compression	Indicates that RTP header compression has been configured for the class.
Sent total	Count of every packet sent, both compressed packets and full-header packets.
Sent compressed	Count of number of compressed packets sent.
bytes saved	Total number of bytes saved (that is, bytes not needing to be sent).
bytes sent	Total number of bytes sent for both compressed and full-header packets.

Field	Description
efficiency improvement factor	The percentage of increased bandwidth efficiency as a result of header compression. For example, with RTP streams, the efficiency improvement factor can be as much as 2.9 (or 290 percent).
hit ratio	Used mainly for troubleshooting purposes, this is the percentage of packets found in the context database. In most instances, this percentage should be high.
five minute miss rate	The number of new traffic flows found in the last five minutes.
misses/sec max	The average number of new traffic flows found per second, and the highest rate of new traffic flows to date.
rate	The actual traffic rate (in bits per second) after the packets are compressed.

Note A number in parentheses may appear next to the service-policy output name and the class-map name. The number is for Cisco internal use only and can be disregarded.

Modular QoS CLI (MQC) Unconditional Packet Discard: Example

The following sample output from the **show policy-map interface** command displays the statistics for the Serial2/0 interface, to which a policy map called "policy1" is attached. The discarding action has been specified for all the packets belonging to a class called "c1." In this example, 32000 bps of traffic is sent ("offered") to the class and all of them are dropped. Therefore, the drop rate shows 32000 bps.

```
Router# show policy-map interface

 Serial2/0
 Serial2/0
  Service-policy output: policy1
    Class-map: c1 (match-all)
       10184 packets, 1056436 bytes
       5 minute offered rate 32000 bps, drop rate 32000 bps
       Match: ip precedence 0
       drop
```

The table below describes the significant fields shown in the display.

Table 239: show policy-map interface Field Descriptions—Configured for MQC Unconditional Packet Discard

Field	Description
Service-policy output	Name of the output service policy applied to the specified interface or VC.
Class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.

Field	Description
packets, bytes	Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
offered rate	Rate, in kbps, of packets coming in to the class. **Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only.
drop rate	Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate.
Note In distributed architecture platforms (such as the Cisco 7500), the value of the transfer rate, calculated as the difference between the offered rate and the drop rate counters, can sporadically deviate from the average by up to 20 percent or more. This can occur while no corresponding burst is registered by independent traffic analyser equipment.	
Match	Match criteria specified for the class of traffic. Choices include criteria such as the Layer 3 packet length, IP precedence, IP DSCP value, MPLS experimental value, access groups, and QoS groups. For more information about the variety of match criteria that are available, see the “Classifying Network Traffic” module in the *Cisco IOS Quality of Service Solutions Configuration Guide* .

Field	Description
drop	Indicates that the packet discarding action for all the packets belonging to the specified class has been configured.

Note A number in parentheses may appear next to the service-policy output name and the class-map name. The number is for Cisco internal use only and can be disregarded.

Percentage-Based Policing and Shaping: Example

The following sample output from the **show policy-map interface** command shows traffic policing configured using a CIR based on a bandwidth of 20 percent. The CIR and committed burst (Bc) in milliseconds (ms) are included in the display.

```
Router# show policy-map interface Serial3/1

  Service-policy output: mypolicy
    Class-map: gold (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      police:
          cir 20 % bc 10 ms
          cir 2000000 bps, bc 2500 bytes
          pir 40 % be 20 ms
          pir 4000000 bps, be 10000 bytes
     conformed 0 packets, 0 bytes; actions:
      transmit
     exceeded 0 packets, 0 bytes; actions:
       drop
      violated 0 packets, 0 bytes; actions:
       drop
      conformed 0 bps, exceed 0 bps, violate 0 bps
```

The table below describes the significant fields shown in the display. A number in parentheses may appear next to the service-policy output name and the class-map name. The number is for Cisco internal use only and can be disregarded.

Table 240: show policy-map interface Field Descriptions—Configured for Percentage-Based Policing and Shaping.

Field	Description
Service-policy output	Name of the output service policy applied to the specified interface or VC.
Class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets, bytes	Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed.

Field	Description
offered rate	Rate, in kbps, of packets coming in to the class. **Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only.
police	Indicates that traffic policing based on a percentage of bandwidth has been enabled. Also, displays the bandwidth percentage, the CIR, and the committed burst (Bc) size in ms.
conformed, actions	Displays the number of packets and bytes marked as conforming to the specified rates, and the action to be taken on those packets.
exceeded, actions	Displays the number of packets and bytes marked as exceeding the specified rates, and the action to be taken on those packets.

Traffic Shaping: Example

The following sample output from the **show policy-map interface** command (shown below) displays the statistics for the serial 3/2 interface. Traffic shaping has been enabled on this interface, and an average rate of 20 percent of the bandwidth has been specified.

Note In HQF images for Cisco IOS Releases 12.4(20)T and later, the packets delayed and bytes delayed counters were removed for traffic shaping classes.

```
Router# show policy-map interface Serial3/2

Serial3/2
  Service-policy output: p1
    Class-map: c1 (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      Traffic Shaping
        Target/Average      Byte   Sustain    Excess      Interval  Increment  Adapt
        Rate              Limit  bits/int  bits/int    (ms)      (bytes)    Active
         20 %                      10 (ms)    20 (ms)
        201500/201500       1952   7808       7808        38         976       -
        Queue     Packets   Bytes     Packets   Bytes     Shaping
        Depth                         Delayed   Delayed   Active
        0         0         0         0         0         no
```

The table below describes the significant fields shown in the display. A number in parentheses may appear next to the service-policy output name, class-map name, and match criteria information. The number is for Cisco internal use only and can be disregarded.

Table 241: show policy-map interface Field Descriptions—Configured for Percentage-Based Policing and Shaping (with Traffic Shaping Enabled).

Field	Description
Service-policy output	Name of the output service policy applied to the specified interface or VC.
Class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets, bytes	Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
offered rate	Rate, in kbps, of packets coming in to the class. **Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only.
drop rate	Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate.
Match	Match criteria specified for the class of traffic. Choices include criteria such as the Layer 3 packet length, IP precedence, IP DSCP value, MPLS experimental value, access groups, and quality of service (QoS) groups. For more information about the variety of match criteria that are available, see the “Classifying Network Traffic” module in the *Quality of Service Solutions Configuration Guide*.
Traffic Shaping	Indicates that traffic shaping based on a percentage of bandwidth has been enabled.
Target/Average Rate	Rate (percentage) used for shaping traffic and the number of packets meeting that rate.
Byte Limit	Maximum number of bytes that can be transmitted per interval. Calculated as follows: ((Bc+Be) /8) x 1
Sustain bits/int	Committed burst (Bc) rate.
Excess bits/int	Excess burst (Be) rate.
Interval (ms)	Time interval value in milliseconds (ms).

Field	Description
Increment (bytes)	Number of credits (in bytes) received in the token bucket of the traffic shaper during each time interval.
Adapt Active	Indicates whether adaptive shaping is enabled.
Queue Depth	Current queue depth of the traffic shaper.
Packets	Total number of packets that have entered the traffic shaper system.
Bytes	Total number of bytes that have entered the traffic shaper system.
Packets Delayed	Total number of packets delayed in the queue of the traffic shaper before being transmitted. **Note** In Cisco IOS Release 12.4(20)T, this counter was removed.
Bytes Delayed	Total number of bytes delayed in the queue of the traffic shaper before being transmitted. **Note** In Cisco IOS Release 12.4(20)T, this counter was removed.
Shaping Active	Indicates whether the traffic shaper is active. For example, if a traffic shaper is active, and the traffic being sent exceeds the traffic shaping rate, a “yes” appears in this field.

Packet Classification Based on Layer 3 Packet Length: Example

The following sample output from the **show policy-map interface** command displays the packet statistics for the Ethernet4/1 interface, to which a service policy called “mypolicy” is attached. The Layer 3 packet length has been specified as a match criterion for the traffic in the class called “class1”.

```
Router# show policy-map interface Ethernet4/1

  Ethernet4/1
  Service-policy input: mypolicy
    Class-map: class1 (match-all)
       500 packets, 125000 bytes
       5 minute offered rate 4000 bps, drop rate 0 bps
       Match: packet length min 100 max 300
       QoS Set
         qos-group 20
           Packets marked 500
```

The table below describes the significant fields shown in the display. A number in parentheses may appear next to the service-policy input name, class-map name, and match criteria information. The number is for Cisco internal use only and can be disregarded.

Table 242: show policy-map interface Field Descriptions—Configured for Packet Classification Based on Layer 3 Packet Length.

Field	Description
Service-policy input	Name of the input service policy applied to the specified interface or VC.

Field	Description
Class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets, bytes	Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
offered rate	Rate, in kbps, of packets coming in to the class. **Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only.
drop rate	Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate.
Match	Match criteria specified for the class of traffic. Choices include criteria such as the Layer 3 packet length, IP precedence, IP DSCP value, MPLS experimental value, access groups, and QoS groups.
QoS Set, qos-group, Packets marked	Indicates that class-based packet marking based on the QoS group has been configured. Includes the qos-group number and the number of packets marked.

Enhanced Packet Marking: Example

The following sample output of the **show policy-map interface** command shows the service policies attached to a FastEthernet subinterface. In this example, a service policy called "policy1" has been attached. In "policy1", a table map called "table-map1" has been configured. The values in "table-map1" will be used to map the precedence values to the corresponding class of service (CoS) values.

```
Router# show policy-map interface

 FastEthernet1/0.1
  Service-policy input: policy1
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      QoS Set
        precedence cos table table-map1
          Packets marked 0
```

The table below describes the fields shown in the display. A number in parentheses may appear next to the service-policy input name and the class-map name. The number is for Cisco internal use only and can be disregarded.

Table 243: show policy-map interface Field Descriptions—Configured for Enhanced Packet Marking.

Field	Description
Service-policy input	Name of the input service policy applied to the specified interface or VC.
Class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets, bytes	Number of the packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
offered rate	Rate, in kbps, of the packets coming into the class.
Match	Match criteria specified for the class of traffic. Choices include criteria such as Precedence, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental value, access groups, and quality of service (QoS) group (set). For more information about the variety of match criteria that are available, see the "Classifying Network Traffic" module in the *Quality of Service Solutions Configuration Guide*.
QoS Set	Indicates that QoS group (set) has been configured for the particular class.
precedence cos table table-map1	Indicates that a table map (called "table-map1") has been used to determine the precedence value. The precedence value will be set according to the CoS value defined in the table map.
Packets marked	Total number of packets marked for the particular class.

Traffic Policing: Example

The following is sample output from the **show policy-map interface** command. This sample displays the statistics for the serial 2/0 interface on which traffic policing has been enabled. The committed (conform) burst (bc) and excess (peak) burst (be) are specified in milliseconds (ms).

```
Router# show policy-map interface serial2/0

 Serial2/0
  Service-policy output: policy1 (1050)
    Class-map: class1 (match-all) (1051/1)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 0  (1052)
      police:
          cir 20 % bc 300 ms
          cir 409500 bps, bc 15360 bytes
          pir 40 % be 400 ms
          pir 819000 bps, be 40960 bytes
        conformed 0 packets, 0 bytes; actions:
```

```
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        violated 0 packets, 0 bytes; actions:
          drop
        conformed 0 bps, exceed 0 bps, violate 0 bps
    Class-map: class-default (match-any) (1054/0)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any  (1055)
        0 packets, 0 bytes
        5 minute rate 0 bps
```

In this example, the CIR and PIR are displayed in bps, and both the committed burst (bc) and excess burst (be) are displayed in bits.

The CIR, PIR bc, and be are calculated on the basis of the formulas described below.

Formula for Calculating the CIR: Example

When calculating the CIR, the following formula is used:

- CIR percentage specified (as shown in the output from the **show policy-map** command) * bandwidth (BW) of the interface (as shown in the output from the**show interfaces** command) = total bits per second

According to the output from the **show interfaces** command for the serial 2/0 interface, the interface has a bandwidth (BW) of 2048 kbps.

```
Router# show interfaces serial2/0

Serial2/0 is administratively down, line protocol is down
  Hardware is M4T
  MTU 1500 bytes, BW 2048 Kbit, DLY 20000 usec, rely 255/255, load 1/255
```

The following values are used for calculating the CIR:

20 % * 2048 kbps = 409600 bps

Formula for Calculating the PIR: Example

When calculating the PIR, the following formula is used:

- PIR percentage specified (as shown in the output from the **show policy-map** command) * bandwidth (BW) of the interface (as shown in the output from the**show interfaces** command) = total bits per second

According to the output from the **show interfaces** command for the serial 2/0 interface, the interface has a bandwidth (BW) of 2048 kbps.

```
Router# show interfaces serial2/0

Serial2/0 is administratively down, line protocol is down
  Hardware is M4T
  MTU 1500 bytes, BW 2048 Kbit, DLY 20000 usec, rely 255/255, load 1/255
```

The following values are used for calculating the PIR:

40 % * 2048 kbps = 819200 bps

Note Discrepancies between this total and the total shown in the output from the **show policy-map interface** command can be attributed to a rounding calculation or to differences associated with the specific interface configuration.

Formula for Calculating the Committed Burst (bc): Example

When calculating the bc, the following formula is used:

- The bc in milliseconds (as shown in the **show policy-map** command) * the CIR in bits per seconds = total number bytes

The following values are used for calculating the bc:

300 ms * 409600 bps = 15360 bytes

Formula for Calculating the Excess Burst (be): Example

When calculating the bc and the be, the following formula is used:

- The be in milliseconds (as shown in the **show policy-map** command) * the PIR in bits per seconds = total number bytes

The following values are used for calculating the be:

400 ms * 819200 bps = 40960 bytes

The table below describes the significant fields shown in the display.

Table 244: show policy-map interface Field Descriptions

Field	Description
Service-policy output	Name of the output service policy applied to the specified interface or VC.
Class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets and bytes	Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
offered rate	Rate, in kbps, of packets coming in to the class.
drop rate	Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate.

Field	Description
Match	Match criteria specified for the class of traffic. Choices include criteria such as the Layer 3 packet length, IP precedence, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental value, access groups, and quality of service (QoS) groups. For more information about the variety of match criteria that are available, see the “Classifying Network Traffic” module in the *Quality of Service Solutions Configuration Guide* .
police	Indicates that traffic policing has been enabled. Display includes the CIR, PIR (in both a percentage of bandwidth and in bps) and the bc and be in bytes and milliseconds. Also displays the optional conform, exceed, and violate actions, if any, and the statistics associated with these optional actions.

Bandwidth Estimation: Example

The following sample output from the **show policy-map interface** command displays statistics for the Fast Ethernet 0/1 interface on which bandwidth estimates for quality of service (QoS) targets have been generated.

The Bandwidth Estimation section indicates that bandwidth estimates for QoS targets have been defined. These targets include the packet loss rate, the packet delay rate, and the timeframe in milliseconds. Confidence refers to the drop-one-in value (as a percentage) of the targets. Corvil Bandwidth means the bandwidth estimate in kilobits per second.

When no drop or delay targets are specified, “none specified, falling back to drop no more than one packet in 500” appears in the output.

```
Router# show policy-map interface FastEthernet0/1

 FastEthernet0/1
  Service-policy output: my-policy
    Class-map: icmp (match-all)
      199 packets, 22686 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: access-group 101
      Bandwidth Estimation:
        Quality-of-Service targets:
          drop no more than one packet in 1000 (Packet loss < 0.10%)
          delay no more than one packet in 100 by 40 (or more) milliseconds
            (Confidence: 99.0000%)
        Corvil Bandwidth: 1 kbits/sec
    Class-map: class-default (match-any)
      112 packets, 14227 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
      Bandwidth Estimation:
        Quality-of-Service targets:
          <none specified, falling back to drop no more than one packet in 500
        Corvil Bandwidth: 1 kbits/sec
```

Shaping with HQF Enabled: Example

The following sample output from the **show policy-mapinterface** command shows that shaping is active (as seen in the queue depth field) with HQF enabled on the serial 4/3 interface. All traffic is classified to the class-default queue.

Note In HQF images for Cisco IOS Releases 12.4(20)T and later, the packets delayed and bytes delayed counters were removed for traffic shaping classes.

```
Router# show policy-map interface serial4/3

 Serial4/3
  Service-policy output: shape
    Class-map: class-default (match-any)
      2203 packets, 404709 bytes
      30 second offered rate 74000 bps, drop rate 14000 bps
      Match: any
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 64/354/0
      (pkts output/bytes output) 1836/337280
      shape (average) cir 128000, bc 1000, be 1000
      target shape rate 128000
        lower bound cir 0,  adapt to fecn 0
      Service-policy : LLQ
        queue stats for all priority classes:

          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
        Class-map: c1 (match-all)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 1
          Priority: 32 kbps, burst bytes 1500, b/w exceed drops: 0
        Class-map: class-default (match-any)
          2190 packets, 404540 bytes
          30 second offered rate 74000 bps, drop rate 14000 bps
          Match: any
          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 63/417/0
          (pkts output/bytes output) 2094/386300
```

Packets Matched on the Basis of VLAN ID Number: Example

Note As of Cisco IOS Release 12.2(31)SB2, matching packets on the basis of VLAN ID numbers is supported on the Catalyst 1000 platform only.

The following is a sample configuration in which packets are matched and classified on the basis of the VLAN ID number. In this sample configuration, packets that match VLAN ID number 150 are placed in a class called “class1.”

```
Router# show class-map

Class Map match-all class1 (id 3)
Match vlan 150
```

Class1 is then configured as part of the policy map called “policy1.” The policy map is attached to Fast Ethernet subinterface 0/0.1.

The following sample output of the **show policy-map interface** command displays the packet statistics for the policy maps attached to Fast Ethernet subinterface 0/0.1. It displays the statistics for policy1, in which class1 has been configured.

```
Router# show policy-map interface

FastEthernet0/0.1
! Policy-map name.
Service-policy input: policy1
! Class configured in the policy map.
Class-map: class1 (match-all)
0 packets, 0 bytes
5 minute offered rate 0 bps, drop rate 0 bps
! VLAN ID 150 is the match criterion for the class.
Match: vlan 150
police:
cir 8000000 bps, bc 512000000 bytes
conformed 0 packets, 0 bytes; actions:
transmit
exceeded 0 packets, 0 bytes; actions:
drop
conformed 0 bps, exceed 0 bps
Class-map: class-default (match-any)
10 packets, 1140 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: any
10 packets, 1140 bytes
5 minute rate 0 bps
```

The table below describes the significant fields shown in the display. A number in parentheses may appear next to the service-policy input name and the class-map name. The number is for Cisco internal use only and can be disregarded.

Table 245: show policy-map interface Field Descriptions—Packets Matched on the Basis of VLAN ID Number.

Field	Description
Service-policy input	Name of the input service policy applied to the specified interface or VC.
Class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets, bytes	Number of the packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
offered rate	Rate, in kbps, of the packets coming into the class.

Field	Description
Match	Match criteria specified for the class of traffic. Choices include criteria such as VLAN ID number, precedence, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental value, access groups, and quality of service (QoS) group (set). For more information about the variety of match criteria that are available, see the “Classifying Network Traffic” module in the *Cisco IOS Quality of Service Solutions Configuration Guide* .

Cisco 7600 Series Routers: Example

The following example shows how to display the statistics and the configurations of all the input and output policies that are attached to an interface on a Cisco 7600 series router:

```
Router# show policy-map interface

 FastEthernet5/36
  service-policy input: max-pol-ipp5
    class-map: ipp5 (match-all)
      0 packets, 0 bytes
      5 minute rate 0 bps
      match: ip precedence 5
  class ipp5
    police 2000000000 2000000 conform-action set-prec-transmit 6 exceed-action p
policed-dscp-transmit
```

The following example shows how to display the input-policy statistics and the configurations for a specific interface on a Cisco 7600 series router:

```
Router# show policy-map interface fastethernet 5/36 input

 FastEthernet5/36
  service-policy input: max-pol-ipp5
    class-map: ipp5 (match-all)
      0 packets, 0 bytes
      5 minute rate 0 bps
      match: ip precedence 5
  class ipp5
    police 2000000000 2000000 conform-action set-prec-transmit 6 exceed-action p
policed-dscp-transmit
```

The table below describes the significant fields shown in the display.

Table 246: show policy-map interface Field Descriptions—Cisco 7600 Series Routers

Field	Description
service-policy input	Name of the input service policy applied to the specified interface.
class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets, bytes	Number of the packets (also shown in bytes) identified as belonging to the class of traffic being displayed.

Field	Description
minute rate	Rate, in kbps, of the packets coming into the class.
match	Match criteria specified for the class of traffic. Choices include criteria such as VLAN ID number, precedence, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental value, access groups, and quality of service (QoS) group (set). For more information about the variety of match criteria that are available, see the "Classifying Network Traffic" module in the *Cisco IOS Quality of Service Solutions Configuration Guide* .
class	Precedence value.
police	Indicates that the **police** command has been configured to enable traffic policing.

Cisco 7200 Series Routers: Example

The following example shows the automatic rounding-off of the **bc** and **be** values, in the MQC police policy-map, to the interface's MTU size in a Cisco 7200 series router. The rounding-off is done only when the bc and be values are lesser than the interface's MTU size.

```
Router# show policy-map interface

Service-policy output: p2
Service-policy output: p2
    Class-map: class-default (match-any)
      2 packets, 106 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: any
        2 packets, 106 bytes
        30 second rate 0 bps
      police:
          cir 10000 bps, bc 4470 bytes
          pir 20000 bps, be 4470 bytes
        conformed 0 packets, 0 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        violated 0 packets, 0 bytes; actions:
          drop
        conformed 0000 bps, exceed 0000 bps, violate 0000 bps
```

Multiple Priority Queues on Serial Interface: Example

The following sample output from the show policy-map interface command shows the types of statistical information that displays when multiple priority queues are configured. Depending upon the interface in use and the options enabled, the output that you see may vary slightly from the output shown below.

```
Router# show policy-map interface

Serial2/1/0
Service-policy output: P1
Queue statistics for all priority classes:
```

```
.
.
.
Class-map: Gold (match-all)
0 packets, 0 bytes   /*Updated for each priority level configured.*/
5 minute offered rate 0 bps, drop rate 0 bps
Match: ip precedence 2
Priority: 0 kbps, burst bytes 1500, b/w exceed drops: 0
Priority Level 4:
0 packets, 0 bytes
```

Bandwidth-Remaining Ratios: Example

The following sample output from the show policy-map interface command indicates that bandwidth-remaining ratios are configured for class queues. As shown in the example, the classes precedence_0, precedence_1, and precedence_2 have bandwidth-remaining ratios of 20, 40, and 60, respectively.

```
Router# show policy-map interface GigabitEthernet1/0/0.10

  Service-policy output: vlan10_policy
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
        0 packets, 0 bytes
        30 second rate 0 bps
      Queueing
      queue limit 250 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      shape (average) cir 1000000, bc 4000, be 4000
      target shape rate 1000000
      bandwidth remaining ratio 10
      Service-policy : child_policy
        Class-map: precedence_0 (match-all)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 0
          Queueing
          queue limit 62 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          shape (average) cir 500000, bc 2000, be 2000
          target shape rate 500000
          bandwidth remaining ratio 20
        Class-map: precedence_1 (match-all)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 1
          Queueing
          queue limit 62 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          shape (average) cir 500000, bc 2000, be 2000
          target shape rate 500000
          bandwidth remaining ratio 40
        Class-map: precedence_2 (match-all)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 2
```

```
    Queueing
    queue limit 62 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 0/0
    shape (average) cir 500000, bc 2000, be 2000
    target shape rate 500000
    bandwidth remaining ratio 60
  Class-map: class-default (match-any)
    0 packets, 0 bytes
    30 second offered rate 0 bps, drop rate 0 bps
    Match: any
      0 packets, 0 bytes
      30 second rate 0 bps

    queue limit 62 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 0/0
```

The table below describes the significant fields shown in the display.

Table 247: show policy-map interface Field Descriptions—Configured for Bandwidth-Remaining Ratios

Field	Description
Service-policy output	Name of the output service policy applied to the specified interface.
Class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets, bytes	Number of the packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
bandwidth remaining ratio	Indicates the ratio used to allocate excess bandwidth.

Tunnel Marking: Example

In this sample output of the **show policy-map interface** command, the character string “ip dscp tunnel 3” indicates that L2TPv3 tunnel marking has been configured to set the DSCP value to 3 in the header of a tunneled packet.

```
Router# show policy-map interface

 Serial0
  Service-policy input: tunnel
    Class-map: frde (match-all)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: fr-de
      QoS Set
        ip dscp tunnel 3
          Packets marked 0
    Class-map: class-default (match-any)
      13736 packets, 1714682 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
        13736 packets, 1714682 bytes
        30 second rate 0 bps
```

The table below describes the significant fields shown in the display.

Table 248: show policy-map interface Field Descriptions—Configured for Tunnel Marking

Field	Description
service-policy input	Name of the input service policy applied to the specified interface.
class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets, bytes	Number of the packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
offered rate	Rate, in kbps, of packets coming in to the class.
drop rate	Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate.
match	Match criteria specified for the class of traffic. In this example, the Frame Relay Discard Eligible (DE) bit has been specified as the match criterion. For more information about the variety of match criteria that are available, see the "Classifying Network Traffic" module in the *Cisco IOS Quality of Service Solutions Configuration Guide*.
ip dscp tunnel	Indicates that tunnel marking has been configured to set the DSCP in the header of a tunneled packet to a value of 3.

Traffic Shaping Overhead Accounting for ATM: Example

The following output from the show policy-map interface command indicates that ATM overhead accounting is enabled for shaping and disabled for bandwidth:

```
Router# show policy-map interface

Service-policy output:unit-test
Class-map: class-default (match-any)
100 packets, 1000 bytes
30 second offered rate 800 bps, drop rate 0 bps
Match: any
shape (average) cir 154400, bc 7720, be 7720
target shape rate 154400
overhead accounting: enabled
bandwidth 30% (463 kbps)
overhead accounting: disabled
queue limit 64 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(packets output/bytes output) 100/1000
```

The table below describes the significant fields shown in the display.

Table 249: show policy-map interface Field Descriptions—Configured for Traffic Shaping Overhead Accounting for ATM

Field	Description
service-policy output	Name of the output service policy applied to the specified interface.
class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets, bytes	Number of the packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
offered rate	Rate, in kbps, of packets coming in to the class.
drop rate	Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate.
match	Match criteria specified for the class of traffic. In this example, the Frame Relay Discard Eligible (DE) bit has been specified as the match criterion. For more information about the variety of match criteria that are available, see the “Classifying Network Traffic” module in the *Cisco IOS Quality of Service Solutions Configuration Guide*.
target shape rate	Indicates that traffic shaping is enabled at the specified rate.
overhead accounting	Indicates whether overhead accounting is enabled or disabled for traffic shaping.
bandwidth	Indicates the percentage of bandwidth allocated for traffic queueing.
overhead accounting:	Indicates whether overhead accounting is enabled or disabled for traffic queueing.

HQF: Example

The following output from the show policy-map interface command displays the configuration for Fast Ethernet interface 0/0:

Note In HQF images for Cisco IOS Releases 12.4(20)T and later releases, the packets delayed and bytes delayed counters were removed for traffic shaping classes.

```
Router# show policy-map interface FastEthernet0/0
 FastEthernet0/0

  Service-policy output: test1

    Class-map: class-default (match-any)
      129 packets, 12562 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
      Queueing
      queue limit 64 packets
```

```
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 129/12562
shape (average) cir 1536000, bc 6144, be 6144
target shape rate 1536000

Service-policy : test2

  queue stats for all priority classes:

    queue limit 64 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 0/0

  Class-map: RT (match-all)
    0 packets, 0 bytes
    30 second offered rate 0 bps, drop rate 0 bps
    Match: ip dscp ef (46)
    Priority: 20% (307 kbps), burst bytes 7650, b/w exceed drops: 0


  Class-map: BH (match-all)
    0 packets, 0 bytes
    30 second offered rate 0 bps, drop rate 0 bps
    Match: ip dscp af41 (34)
    Queueing
    queue limit 128 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 0/0
    bandwidth 40% (614 kbps)

  Class-map: BL (match-all)
    0 packets, 0 bytes
    30 second offered rate 0 bps, drop rate 0 bps
    Match: ip dscp af21 (18)
    Queueing
    queue limit 64 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 0/0
    bandwidth 35% (537 kbps)
      Exp-weight-constant: 9 (1/512)
      Mean queue depth: 0 packets
      dscp     Transmitted    Random drop    Tail drop   Minimum    Maximum    Mark
               pkts/bytes     pkts/bytes     pkts/bytes  thresh     thresh     prob

      af21     0/0            0/0            0/0         100        400        1/10

  Class-map: class-default (match-any)
    129 packets, 12562 bytes
    30 second offered rate 0 bps, drop rate 0 bps
    Match: any

    queue limit 64 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 129/12562
```

The table below describes the significant fields shown in the display.

Table 250: show policy-map interface Field Descriptions—Configured for HQF

Field	Description
FastEthernet	Name of the interface.

Field	Description
service-policy output	Name of the output service policy applied to the specified interface.
class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets, bytes	Number of the packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
offered rate	Rate, in kbps, of packets coming in to the class.
drop rate	Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate.
Match	Match criteria specified for the class of traffic. **Note** For more information about the variety of match criteria that are available, see the "Classifying Network Traffic" module in the *Cisco IOS Quality of Service Solutions Configuration Guide*.
Queueing	Indicates that queueing is enabled.
queue limit	Maximum number of packets that a queue can hold for a class policy configured in a policy map.
bandwidth	Indicates the percentage of bandwidth allocated for traffic queueing.
dscp	Differentiated services code point (DSCP). Values can be the following: • 0 to 63—Numerical DSCP values. The default value is 0. • af1 to af43—Assured forwarding (AF) DSCP values. • cs1 to cs7—Type of service (ToS) precedence values. • default—Default DSCP value. • ef—Expedited forwarding (EF) DSCP values.

Account QoS Statistics for the Cisco ASR 1000 Series Aggregation Services Routers: Example

The following example shows the new output fields associated with the QoS: Policies Aggregation Enhancements feature beginning in Cisco IOS XE Release 2.6 for subscriber statistics. The new output fields begin with the label "Account QoS Statistics."

```
Router# show policy-map interface port-channel 1.1

Port-channel1.1
   Service-policy input: input_policy
     Class-map: class-default (match-any)
       0 packets, 0 bytes
       5 minute offered rate 0000 bps, drop rate 0000 bps
```

```
      Match: any
      QoS Set
      dscp default
      No packet marking statistics available
  Service-policy output: Port-channel_1_subscriber
    Class-map: EF (match-any)
      105233 packets, 6734912 bytes
      5 minute offered rate 134000 bps, drop rate 0000 bps
      Match: dscp ef (46)
      Match: access-group name VLAN_REMARK_EF
      Match: qos-group 3
      Account QoS statistics
        Queueing
          Packets dropped 0 packets/0 bytes
      QoS Set
      cos 5
      No packet marking statistics available
      dscp ef
      No packet marking statistics available
    Class-map: AF4 (match-all)
      105234 packets, 6734976 bytes
      5 minute offered rate 134000 bps, drop rate 0000 bps
      Match: dscp cs4 (32)
      Account QoS statistics
        Queueing
          Packets dropped 0 packets/0 bytes
      QoS Set
      cos 4
      No packet marking statistics available
    Class-map: AF1 (match-any)
      315690 packets, 20204160 bytes
      5 minute offered rate 402000 bps, drop rate 0000 bps
      Match: dscp cs1 (8)
      Match: dscp af11 (10)
      Match: dscp af12 (12)
      Account QoS statistics
        Queueing
          Packets dropped 0 packets/0 bytes
      QoS Set
      cos 1
      No packet marking statistics available
    Class-map: class-default (match-any) fragment Port-channel_BE
      315677 packets, 20203328 bytes
      5 minute offered rate 402000 bps, drop rate 0000 bps
      Match: any
      Queueing
        queue limit 31250 bytes
        (queue depth/total drops/no-buffer drops) 0/0/0
        (pkts output/bytes output) 315679/20203482
        bandwidth remaining ratio 1
```

Cisco Catalyst 4000 Series Routers: Example

The following example shows how to display the policer statistics (the packet and byte count). The output displays only the applicable count (either packets or bytes) with the actual number.

```
Router# show policy-map interface GigabitEthernet 3/1 input

GigabitEthernet3/1
  Service-policy input: in1
    Class-map: p1 (match-all)
```

```
      0 packets
      Match:  precedence 1
           QoS Set
             ip precedence 7
      police:
          cir 20 %
          cir 200000000 bps, bc 6250000 bytes
        conformed 0 bytes; actions:
          transmit
        exceeded 0 bytes; actions:
          drop
        conformed 0000 bps, exceed 0000 bps
    Class-map: class-default (match-any)
      10000000 packets
      Match: any
      police:
          cir 20 %
          cir 200000000 bps, bc 6250000 bytes
        conformed 174304448 bytes; actions:
          transmit
        exceeded 465695552 bytes; actions:
          drop
        conformed 4287000 bps, exceed 11492000 bps
```

Cisco CMTS Routers: Example

The following example shows how to display the statistics and the configurations of the input and output service policies that are attached to an interface:

```
Router# show policy-map interface GigabitEthernet 1/2/0

Load for five secs: 1%/0%; one minute: 1%; five minutes: 1%
Time source is hardware calendar, *23:02:40.857 pst Thu Mar 3 2011

 GigabitEthernet1/2/0

  Service-policy input: policy-in

    Class-map: class-exp-0 (match-all)
      6647740 packets, 9304674796 bytes
      30 second offered rate 3234000 bps, drop rate 0 bps
      Match: mpls experimental topmost 0
      QoS Set
        precedence 3
          Packets marked 6647740

    Class-map: class-default (match-any)
      1386487 packets, 1903797872 bytes
      30 second offered rate 658000 bps, drop rate 0 bps
      Match: any

  Service-policy output: policy-out

    Class-map: class-pre-1 (match-all)
      2041355 packets, 2857897000 bytes
      30 second offered rate 986000 bps, drop rate 0 bps

      Match: ip precedence 1
      QoS Set
        mpls experimental topmost 1
          Packets marked 2041355
```

```
    Class-map: class-default (match-any)
      6129975 packets, 8575183331 bytes
      30 second offered rate 2960000 bps, drop rate 0 bps
      Match: any
```

The table below describes the significant fields shown in the display.

Table 251: show policy-map interface Field Descriptions—Cisco Catalyst 4000 Series Routers

Field	Description
class-map	Displays the class of traffic. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
conformed	Displays the action to be taken on packets conforming to a specified rate. Also displays the number of packets and bytes on which the action was taken.
drop	Indicates that the packet discarding action for all the packets belonging to the specified class has been configured.
exceeded	Displays the action to be taken on packets exceeding a specified rate. Displays the number of packets and bytes on which the action was taken.
match	Match criteria specified for the class of traffic.
packets, bytes	Number of the packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
police	Indicates that the **police** command has been configured to enable traffic policing. Also displays the specified CIR, conform burst size, peak information rate (PIR), and peak burst size used for marking packets.
QoS Set	Indicates that QoS group (set) has been configured for the particular class.
service-policy input	Name of the input service policy applied to the specified interface.

Displaying Pseudowire Policy Map Information: Example

The following example shows how to display the class maps configured for a pseudowire interface:

```
Router# show policy-map interface pseudowire2
 pseudowire2
  Service-policy output: pw_brr

    Class-map: prec1 (match-all)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: ip precedence 1
      Queueing
      queue limit 4166 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth remaining ratio 1
```

```
    Class-map: prec2 (match-all)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: ip precedence 2
      Queueing
      queue limit 4166 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth remaining ratio 2

    Class-map: prec3 (match-all)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: ip precedence 3
      Queueing
      queue limit 4166 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth remaining ratio 3

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: any
      Queueing
      queue limit 4166 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth remaining ratio 4
Device#
```

The table below describes the significant fields shown in the display.

Table 252: show policy-map interface Field Descriptions—Pseudowire Policy Map Information

Field	Description
bandwidth	Indicates the percentage of bandwidth allocated for traffic queueing.
Class-map	Displays the class of traffic. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
Match	Match criteria specified for the class of traffic.
packets, bytes	Number of the packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
Queueing	Indicates that queueing is enabled.
queue limit	Maximum number of packets that a queue can hold for a class policy configured in a policy map.
service-policy output	Name of the output service policy applied to the specified interface.

Related Commands

Command	Description
bandwidth remaining ratio	Specifies a bandwidth-remaining ratio for class queues and subinterface-level queues to determine the amount of unused (excess) bandwidth to allocate to the queue during congestion.
class-map	Creates a class map to be used for matching packets to a specified class.
compression header ip	Configures RTP or TCP IP header compression for a specific class.
drop	Configures a traffic class to discard packets belonging to a specific class.
match fr-dlci	Specifies the Frame Relay DLCI number as a match criterion in a class map.
match packet length (class-map)	Specifies the length of the Layer 3 packet in the IP header as a match criterion in a class map.
police	Configures traffic policing.
police (percent)	Configures traffic policing on the basis of a percentage of bandwidth available on an interface.
police (two rates)	Configures traffic policing using two rates, the CIR and the PIR.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
priority	Specifies that low-latency behavior must be given to a traffic class and configures multiple priority queues.
random-detect ecn	Enables ECN.
shape (percent)	Specifies average or peak rate traffic shaping on the basis of a percentage of bandwidth available on an interface.
show class-map	Display all class maps and their matching criteria.
show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.
show interfaces	Displays statistics for all interfaces configured on a router or access server.
show mls qos	Displays MLS QoS information.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map class	Displays the configuration for the specified class of the specified policy map.
show table-map	Displays the configuration of a specified table map or of all table maps.

Command	Description
table-map (value mapping)	Creates and configures a mapping table for mapping and converting one packet-marking value to another.

show power

To display information about the power status, use the **show power**command in user EXEC or privileged EXEC mode**.**

show power [{**available** | **inline** [{*interface number* | **module number**}] | **redundancy-mode** | **status** {**all** | **fan-tray** *fan-tray-number* | **module** *slot* | **power-supply** *pwr-supply-number*} | **total** | **used**}]

Syntax Description

available	(Optional) Displays the available system power (margin).
inline	(Optional) Displays the inline power status.
interface number	(Optional) Specifies the interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **null**, **port-channel**, and **vlan**. See the "Usage Guidelines" section for additional information.
module number	Displays the power status for a specific module.
redundancy-mode	(Optional) Displays the power-supply redundancy mode.
status	(Optional) Displays the power status.
all	Displays all the FRU types.
fan-tray *fan-tray-number*	Displays the power status for the fan tray .
module *slo* t	Displays the power status for a specific module.
power-supply *pwr-supply-number*	Displays the power status for a specific power supply; valid values are **1** and **2**
total	(Optional) Displays the total power that is available from the power supplies.
used	(Optional) Displays the total power that is budgeted for powered-on items.

Command Default

This command has no default settings.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX1	The output was changed to include the total system-power information.
12.2(17b)SXA	This command was changed to include information about the inline power status for a specific module.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.

Release	Modification
12.2(18)SXF	The output was changed to include information about the high-capacity power supplies.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

Valid values for *vlan-id* are from 1 to 4094.

The Inline power field in the **show power**output displays the inline power that is consumed by the modules. For example, this example shows that module 9 has consumed 0.300 A of inline power:

```
Inline power   #    current
module         9    0.300A
```

Examples

This example shows how to display the available system power:

```
Router>
show power
available
system power available = 20.470A
Router>
```

This example shows how to display power-supply redundancy mode:

```
Router#
show power
redundancy-mode
system power redundancy mode = redundant
Router#
```

This command shows how to display the system-power status:

```
Router> show power
system power redundancy mode = combined
system power total =     3984.12 Watts (94.86 Amps @ 42V)
system power used =      1104.18 Watts (26.29 Amps @ 42V)
system power available = 2879.94 Watts (68.57 Amps @ 42V)
                        Power-Capacity PS-Fan Output Oper
PS   Type               Watts   A @42V Status Status State
---- ------------------ ------- ------ ------ ------ -----
1    WS-CAC-3000W       2830.80 67.40  OK     OK     on
2    WS-CAC-1300W       1153.32 27.46  OK     OK     on
Note: PS2 capacity is limited to 2940.00 Watts (70.00 Amps @ 42V)
      when PS1 is not present
                        Pwr-Allocated  Oper
Fan  Type               Watts   A @42V State
---- ------------------ ------- ------ -----
1    FAN-MOD-9           241.50  5.75  OK
2                        241.50  5.75  failed
```

```
                         Pwr-Requested  Pwr-Allocated  Admin Oper
Slot Card-Type           Watts   A @42V Watts   A @42V State State
---- ------------------ ------- ------ ------- ------ ----- -----
1    WS-X6K-SUP2-2GE     145.32  3.46   145.32  3.46  on    on
2                          -      -     145.32  3.46  -     -
3    WS-X6516-GBIC       118.02  2.81   118.02  2.81  on    on
5    WS-C6500-SFM        117.18  2.79   117.18  2.79  on    on
7    WS-X6516A-GBIC      214.20  5.10     -      -    on    off (insuff cooling capacity)
8    WS-X6516-GE-TX      178.50  4.25   178.50  4.25  on    on
9    WS-X6816-GBIC       733.98 17.48     -      -    on    off (connector rating exceeded)
Router>
```

This example shows how to display the power status for all FRU types:

```
Router#
show power
status all
FRU-type       #    current   admin state oper
power-supply   1    27.460A   on          on
module         1    4.300A    on          on
module         2    4.300A    -           -   (reserved)
module         5    2.690A    on          on
Router#
```

This example shows how to display the power status for a specific module:

```
Router#
show power
status module 1
FRU-type       #    current   admin state oper
module         1    -4.300A   on          on
Router#
```

This example shows how to display the power status for a specific power supply:

```
Router#
show power
status power-supply 1
FRU-type       #    current   admin state oper
power-supply   1    27.460A   on          on
Router#
```

This example displays information about the high-capacity power supplies:

```
Router#
show power
status power-supply 2
                         Power-Capacity PS-Fan Output Oper
PS   Type                Watts   A @42V Status Status State
---- ------------------ ------- ------ ------ ------ -----
1    WS-CAC-6000W        2672.04  63.62 OK     OK     on
2    WS-CAC-9000W-E      2773.68  66.04 OK     OK     on
Router#
```

This example shows how to display the total power that is available from the power supplies:

```
Router#
show power
total
system power total = 27.460A
Router#
```

This example shows how to display the total power that is budgeted for powered-on items:

```
Router#
show power
used
system power used = -6.990A
Router#
```

This command shows how to display the inline power status on the interfaces:

```
Router#
show power
inline
Interface            Admin    Oper     Power ( mWatt )  Device
-------------------- ----- ---------- --------------- -----------
FastEthernet9/1      auto  on         6300            Cisco 6500 IP Phone
FastEthernet9/2      auto  on         6300            Cisco 6500 IP Phone
.
.
. <Output truncated>
```

This command shows how to display the inline power status for a specific module:

```
Router
# show power
inline mod 7

Interface  Admin    Oper     Power       Device         Class
                             (Watts)
---------- ----- ---------- ------- --------------  -----------
Gi7/1      auto   on            6.3  Cisco IP Phone 7960  n/a
Gi7/2      static power-deny      0  Ieee PD               3
.
.
. <Output truncated>
```

Related Commands

Command	Description
power enable	Turns on power for the modules.
power redundancy-mode	Sets the power-supply redundancy mode.

show power inline

To display the power status for a specified port or for all ports, use the **show power inline** command in privileged EXEC mode.

show power inline [*interface-type slot/port*] [{**actual** | **configured**}]

Syntax Description

interface -type	(Optional) Type of interface.
slot	(Optional) Slot number.
/ *port*	(Optional) Port number.
actual	(Optional) Displays the present power status, which might not be the same as the configured power.
configured	(Optional) Displays the configured power status.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XU	This command was introduced.
12.2(2)XT	This command was introduced on the Cisco 2600 series, the Cisco 3600 series, and the Cisco 3700 series routers to support switchport creation.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T to support switchport creation on Cisco 2600 series, the Cisco 3600 series, and Cisco 3700 series routers.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE 3.9S	This command was integrated into Cisco IOS Release XE 3.9S.

Usage Guidelines

The **show power inline** command displays the amount of power used to operate a Cisco IP phone. To view the amount of power requested, use the **show cdp neighbors** command.

Use the **show power inline** *gigabitEthernet* **detail** command on a Cisco 4400 Series Integrated Services Router (ISR) to monitor the total available power budget on your router.

Examples

The following is sample output from the **show power inlinefa0**/**4actual** command asking for the actual status of each interface rather than what is configured for each:

```
Router#
show power inline fastethernet 0/4 actual
Interface            Power
-------------------- -----
FastEthernet0/4      no
```

Notice that the status shown for the FastEthernet interface 0/4, there is no power.

Cisco 4400 Series Integrated Services Router (ISR): Example

The following are sample outputs from the **show power inline** command and the **show power inline** *gigabitEthernet* **detail** commands

```
 Router# show power inline

Available:31.0(w)  Used:30.8(w)  Remaining:0.2(w)

Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Gi0/0/0   auto   on         15.4    Ieee PD             4     30.0
Gi0/0/1   auto   on         15.4    Ieee PD             4     30.0
```

```
Router# show power inline gigabitEthernet 0/0/0 detail
Interface: Gi0/0/0
 Inline Power Mode: auto
 Operational status: on
 Device Detected: yes
 Device Type: Ieee PD
 IEEE Class: 4
 Discovery mechanism used/configured: Ieee
 Police: off

 Power Allocated
 Admin Value: 30.0
 Power drawn from the source: 15.4
 Power available to the device: 15.4

 Absent Counter: 0
 Over Current Counter: 0
 Short Current Counter: 0
 Invalid Signature Counter: 0
 Power Denied Counter: 0
```

Related Commands

Command	Description
power inline	Determines how inline power is applied to devices on the specified Fast Ethernet port.
show cdp neighbors	Displays detailed information about neighboring devices discovered using CDP.

show proc cpu platform

To display detailed CPU usage statistics for platform processes in relation to the Control Processor (CP), Service Processor (SP), or Data Processor (DP), use the **show proc cpu platform** command. This command now includes filtering options based on CP, SP, or DP, and can be sorted by time duration (1min, 5min, 5sec) to provide more specific output.

show process cpu platform [{ **control-plane** | **data-plane** | **service-plane** }]

Syntax Description

proc	Specifies process.
cpu	Specifies CPU.
platform	Specifies platform.
control-plane	(Optional) Specifies the control plane of the router. The control plane is responsible for routing operations and other control functions.
data-plane	(Optional) Specifies the data plane of the router. The data plane is responsible for processing and forwarding data packets.
service-plane	(Optional) Specifies the service plane of the router. The service plane handles services such as management and configuration interfaces.

Command Default

There is no default.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 17.13.1a	The command was updated to include CP, SP, DP filters in the CLI. When these filters are specified by the user, the output is specific to the respective plane.

Usage Guidelines

The **show process cpu platform** command can provide detailed information on a core-by-core basis. This can be useful for getting a detailed view of your system's operation, but it might not always provide a clear picture of the overall system health.

For information about the overall system health, the recommended command is **show platform resources.**

The following example shows the detailed CPU usage statistics for platform processes related to the Control Processor

```
Router#show proc cpu plat sort
CPU utilization for five seconds:  8%, one minute:  7%, five minutes: 10%
Core 0: CPU utilization for five seconds: 12%, one minute:  4%, five minutes: 10%
Core 1: CPU utilization for five seconds: 12%, one minute:  3%, five minutes:  9%
Core 2: CPU utilization for five seconds:  0%, one minute:  0%, five minutes:  3%
Core 3: CPU utilization for five seconds:  0%, one minute:  0%, five minutes:  7%
Core 4: CPU utilization for five seconds:  0%, one minute:  0%, five minutes:  7%
Core 5: CPU utilization for five seconds:  0%, one minute:  0%, five minutes:  5%
Core 6: CPU utilization for five seconds: 10%, one minute:  6%, five minutes:  5%
```

```
Core 7: CPU utilization for five seconds:  6%, one minute:  3%, five minutes:  6%
Core 8: CPU utilization for five seconds: 28%, one minute: 15%, five minutes:  9%
Pid    PPid    5Sec    1Min    5Min  Status        Size  Name
--------------------------------------------------------------------------------
 17295   17288    166%    162%    116%  S           862100  ucode_pkt_PPE0
  8731    8722      3%      2%      8%  S           871892  linux_iosd-imag
 22924   22918      1%      0%      3%  S            14280  ngiolite
 17198   17187      1%      1%      1%  S           156380  fman_fp_image
 29497   29491      0%      0%      0%  S             2684  iox_restart.sh
 29491    8045      0%      0%      0%  S             2692  pman
```

Note The numbers reported are sourced from Linux and represent the specialized ways in which the CPU cores are being used from the kernel's perspective. The numbers can be high as the overall kernel CPU usage is typically high. The ucode_pkt_PPE0 process, which represents the sum of all threats, usually shows high utilization. It's important to note that this is not scaled to 100% and can exceed that number.

show process | include persis

To verify the validity of the process during alarm history configuration, use the **show process | include persis** command.

Syntax Description

Syntax Description

Command Default

There is no default.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
XE 3.18 SP	Support for this command was introduced on NCS 4200 Series.

Examples

The following example shows the detailed information about a particular circuit.:

```
Router#show process | include persis
292 Msi 13F0D4AC 0 49 010328/12000 0 mcprp_spa_persis
```

show protection-group

Use this command to verify the protection group configuration. It defines the status of the protection group.

show protection-group

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1	Support for this command was introduced for the Cisco NCS 4200 Series and Cisco ASR 900 Series Routers.

Usage Guidelines

This command is used for configuring protection group parameters.

Examples

The following example shows how to configure protection group:

```
show protection-group
PGN Type Working I/f Protect I/f Active Status
--------------------------------------------------------------------------------
401 STS48C SONET0/3/6.1-48 SONET0/12/6.1-48 W A
--------------------------------------------------------------------------------
Status legend:D=Deleted FO=Force SF=SignalFailure SD=SignalDegrade
FL=Fail M=Manual L=Lockout C=Clear A=Auto
(W)=working, (P)=protect
```

Related Commands

Command	Description
controller protection-group	Configures protection group controller.
protection-group	Configures virtual protection group interface.
protection-group *group id* [**working** | **protect**]	Configures protection group roles.

show ptp clock dataset

To display a summary of the Precision Time Protocol clock status, use the show ptp clock dataset command in privileged EXEC mode.

show ptp clock dataset [{**default** | **current**}]

Cisco ASR 901 Series Aggregation Services Router

show ptp clock dataset {**default** | **current**}

Syntax Description

default	(Optional) Displays the default PTP clock dataset. **Note** **default** On the ASR 901 Series Aggregation Services Router, you must choose either the**default** keyword or the **current** keyword.
current	(Optional) Displays the current PTP clock dataset. **Note** On the ASR 901 Series Aggregation Services Router, you must choose either the**current** keyword or the **default** keyword.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)S	This command was introduced.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

Use this command to verify a PTP clocking configuration.

On the Cisco ASR 901 Series Aggregation Services Router, one of the keywords (**default** or **current**) must be used with the command.

Examples

The following examples show the output generated by this command:

```
Device# show ptp clock dataset default

CLOCK [Boundary Clock, domain 10]
  Two Step Flag: No
  Clock Identity: 0x2A:0:0:0:58:67:F3:4
  Number Of Ports: 1
  Priority1: 89
  Priority2: 90
  Domain Number: 10
  Slave Only: No
  Clock Quality:
    Class: 224
    Accuracy: Unknown
    Offset (log variance): 4252
```

```
Device# show ptp clock dataset current

CLOCK [Boundary Clock, domain 10]
  Steps Removed: 18522
  Offset From Master: 4661806827187470336
  Mean Path Delay: 314023819427708928
```

The table below describes significant fields shown in the display.

Table 253: show ptp clock dataset Field Descriptions

Field	Description
Two Step Flag	Indicates whether the clock is sending timestamp information using a FOLLOW_UP message (a 2-step handshake) or not (a 1-step handshake).
Clock Identity	Unique identifier for the clock.
Number of Ports	Number of ports assigned to the PTP clock.
Priority1	Priority1 preference value of the PTP clock; the priority1 clock is considered first during clock selection.
Priority2	Priority2 preference value of the PTP clock; the priority2 clock is considered after all other clock sources during clock selection.
Domain number	PTP clocking domain number.
Slave only	Specifies whether the PTP clock is a slave-only clock.
Clock quality	Summarizes the quality of the grandmaster clock.
Class	Displays the time and frequency traceability of the grandmaster clock
Accuracy	Field applies only when the Best Master Clock algorithm is in use; indicates the expected accuracy of the primary clock were the grandmaster clock.
Offset (log variance)	Offset between the local clock and an ideal reference clock.
Steps removed	Number of hops from the local clock to the grandmaster clock.
Offset From Master	Time offset between the subordinate and primary clocks.
Mean Path Delay	Mean propagation time between the primary and subordinate clocks.

show ptp clock dataset parent

To display a description of the Precision Time Protocol parent clock, use the show ptp dataset parent command in privileged EXEC mode.

show ptp clock dataset parent

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)S	This command was introduced.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

Use this command to verify a PTP clocking configuration.

Examples

The following example shows the output generated by this command:

```
Device# show ptp clock dataset parent

CLOCK [Boundary Clock, domain 10]
  Parent Stats: No
  Observed Parent Offset (log variance): 0
  Observed Parent Clock Phase Change Rate: 58087144
  Grandmaster Clock:
    Identity: 0x3E:D3:D0:0:0:0:0:0
    Priority1: 42
    Priority2: 0
    Clock Quality:
      Class: 176
      Accuracy: Unknown
      Offset (log variance): 4252
```

The table below describes significant fields shown in the display.

Table 254: show ptp clock dataset parent Field Descriptions

Field	Description
Parent Stats	Indicates the availability of parent statistics.
Observed Parent Offset (log variance)	The offset between the parent clock and the local clock.
Observed Parent Clock Phase Change Rate	This value indicates the parent clock speed relative to the subordinate clock. A positive value indicates that the parent clock is faster than the subordinate clock ; a negative value indicates that the parent clock is slower than the subordinate clock.
Grandmaster clock	Summarizes the Grandmaster clock configuration.

Field	Description
Identity	The hardware address of the Grandmaster clock.
Priority1	The priority1 preference value of the PTP clock; the priority1 clock is considered first during clock selection.
Priority2	The priority2 preference value of the PTP clock; the priority2 clock is considered after all other clock sources during clock selection.
Clock Quality	Summarizes the quality of the Grandmaster clock.
Class	Displays the time and frequency traceability of the grandmaster clock
Accuracy	This field applies only when the Best Master Clock algorithm is in use; indicates the expected accuracy of the primary clock were the grandmaster clock.
Offset (log variance)	The offset between the Grandmaster clock and the parent clock.

show ptp clock dataset time-properties

To display a summary of time properties for a Precision Time Protocol clock, use the show ptp dataset time-properties command in privileged EXEC mode.

show ptp clock dataset time-properties

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)S	This command was introduced.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

Use this command to verify a PTP clocking configuration.

Examples

The following example shows the output generated by this command:

```
Device# show ptp clock dataset time-properties

CLOCK [Boundary Clock, domain 10]
  Current UTC Offset Valid: TRUE
  Current UTC Offset: 10752
  Leap 59: FALSE
  Leap 61: TRUE
  Time Traceable: TRUE
  Frequency Traceable: TRUE
  PTP Timescale: TRUE
  Time Source: Unknown
```

The table below describes significant fields shown in the display.

Table 255: show ptp clock dataset time-properties Field Descriptions

Field	Description
Current UTC Offset Valid	Indicates whether the current UTC offset is valid.
Current UTC Offset	Offset between the TAI and UTC in seconds.
Leap 59	Indicates whether the last minute of the current UTC day contains 59 seconds.
Leap 61	Indicates whether the last minute of the current UTC day contains 61 seconds.
Time Traceable	Indicates whether the value of the current UTC offset is traceable to a primary reference.
Frequency Traceable	Indicates whether the frequency used to determine the time scale is traceable to a primary reference.

Field	Description
PTP Timescale	Indicates whether the PTP grandmaster clock uses a PTP clock time scale.
Time Source	Time source used by the grandmaster clock.

show ptp clock running

To display a summary of the Precision Time Protocol clock status, use the show ptp clock running command in privileged EXEC mode.

show ptp clock running [**domain**]

Syntax Description

domain	Filters output by domain.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)S	This command was introduced.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

Use this command to verify a PTP clocking configuration.

Examples

The following example shows the output generated by this command:

```
Device# show ptp clock running

PTP Boundary Clock [Domain 1]
         State          Ports          Pkts sent      Pkts rcvd
         FREERUN        3              1090           1023
                               PORT SUMMARY
Name               Tx Mode      Role         Transport    State         Sessions
MASTER-1           unicast      master       Et0/0        -             5
MASTER-2           mcast        master       Et0/0        -             5
SLAVE              unicast      slave        Et0/0        -             5
                      PTP Ordinary Clock [Domain 2]
         State          Ports          Pkts sent      Pkts rcvd
         HOLDOVER       1              2090           2023
                               PORT SUMMARY
Name               Tx Mode      Role         Transport    State         Sessions
MASTER             unicast      master       Et0/0        -             5
```

The table below describes significant fields shown in the display.

Table 256: show ptp clock running Field Descriptions

Field	Description
State	State of the PTP clock.
Ports	Number of ports assigned to the PTP clock.
Pkts sent	Number of packets sent by the PTP clock.
Pkts rcvd	Number of packets received by the PTP clock.

Field	Description
Name	Name of the PTP clock port.
Tx Mode	Transmission mode of the PTP clock port (unicast or multicast).
Role	PTP role of the clock port (primary or subordinate).
Transport	Physical port assigned to the clock port.
State	State of the clock port.
Sessions	Number of PTP sessions active on the clock port.

show ptp port dataset foreign-master

To display a summary of Precision Time Protocol foreign master records, use the **show ptp port dataset foreign-master-record** command in privileged EXEC mode.

show ptp port dataset foreign-master [**domain**]

Syntax Description

This command has no arguments or keywords.

domain	Filters output by domain.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)S	This command was introduced.

Usage Guidelines

Use this command to verify a PTP clocking configuration.

Examples

The following example shows the output generated by this command.

```
Device# show ptp dataset foreign-master

PTP FOREIGN MASTER RECORDS
Interface Vlan2
Number of foreign records 1, max foreign records 5
Best foreign record 0
RECORD #0
Foreign master port identity: clock id: 0x0:1E:4A:FF:FF:96:A2:A9
Foreign master port identity: port num: 1
Number of Announce messages: 8
Number of Current Announce messages: 6
Time stamps: 1233935406, 664274927
```

The table below describes significant fields shown in the display.

Table 257: show ptp port dataset foreign-master Field Descriptions

Field	Description
Interface	Currently foreign-master data is not displayed in the show command.
Number of foreign records	Number of foreign master records in device memory.
max foreign records	Maximum number of foreign records.
Best foreign record	Foreign record with the highest clock quality.
Foreign master port identity: clock id	Hardware address of the foreign master port.
Foreign master port identity: port number	Port number of the foreign master port.

Field	Description
Number of Announce messages	Number of Announce messages received from the foreign master clock.
Number of Current Announce messages	Number of current announcement messages.
Time stamps	Time stamps of current announcement messages.

show ptp port dataset port

To display a summary of Precision Time Protocol ports, use the **show ptp port dataset port** command in privileged EXEC mode.

show ptp dataset port

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)S	This command was introduced.

Usage Guidelines

Use this command to verify a PTP clocking configuration.

Examples

The following example shows the output generated by this command.

```
Device# show ptp port dataset port

PORT [MASTER]
  Clock Identity: 0x49:BD:D1:0:0:0:0:0
  Port Number: 0
  Port State: Unknown
  Min Delay Req Interval (log base 2): 42
  Peer Mean Path Delay: 648518346341351424
  Announce interval (log base 2): 0
  Announce Receipt Timeout: 2
  Sync Interval (log base 2): 0
  Delay Mechanism: End to End
  Peer Delay Request Interval (log base 2): 0
  PTP version: 2
```

The table below describes significant fields shown in the display.

Table 258: show ptp port dataset port Field Descriptions

Field	Description
Clock Identity	Unique identifier for the clock.
Port Number	Port number on the PTP node.
Port State	State of the PTP port.
Min Delay Req Interval (log base 2)	Time interval permitted between Delay_Req messages.
Peer Mean Path Delay	One way propagation delay on the local port.
Announce interval (log base 2)	Mean interval between PTP announcement messages.
Announce Receipt Timeout	Number of intervals before a PTP announcement times out.

Field	Description
Sync Interval (log base 2)	Mean interval between PTP sync messages.
Delay Mechanism	Mechanism used for measuring propagation delay.
Peer Delay Request Interval (log base 2)	Interval permitted between Peer Delay Request messages.
PTP version	PTP version in use.

show pxf cpu access-lists

To display Parallel eXpress Forwarding (PXF) memory information for access control lists (ACLs), use the **show pxf cpu access-lists** command in privileged EXEC mode.

show pxf cpu access-lists [{**security** | **qos** | **pbr** | **compiled**}]

Cisco 10000 Series Router
show pxf cpu access-lists [{**security** [{[**tcam** *acl-name* [**detail**]] | **flex-sum** | **children**}] | **qos** | **pbr** | **compiled**}]

Syntax Description

security	(Optional) Displays information about the security ACLs defined in Cisco IOS and compiled to the PXF. Also displays information about split ACLs, such as how much memory has been used.
tcam *acl-name*	(Optional) Displays information about the specified security ACL stored in ternary content addressable memory (TCAM). This option is only available on the PRE3 for the Cisco 10000 series router.
detail	(Optional) Displays decoded information about the packet fields used for matching in the TCAM.
flex-sum	(Optional) Displays summary information describing the amount of memory allocated in the parallel express forwarding (PXF) engine for use by the flexible key construction microcode. This information is useful for design teams. This option is only available on the PRE3 for the Cisco 10000 series router.
children	(Optional) Displays information for child policies. If an ACL is a template child, the output typically does not display the child information. Specifying the **children** keyword displays data for child policies, too, and shows the children and the parent policy of each child. Use caution when using the **children** keyword as there might be thousands of child policies configured, which could have negative effects on the command output.
qos	(Optional) Displays information about the QoS ACLs defined in Cisco IOS and compiled to the PXF.
pbr	(Optional) Displays information about ACLs for policy-based routing (PBR).
compiled	(Optional) Displays information for all compiled Turbo-ACLs. The PRE2 supports Turbo-ACLs and the **compiled** option. The PRE3 accepts the PRE2 **compiled** option, but does not implement Turbo-ACLs.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2S	This command was introduced.
12.3(7)XI1	This command was introduced on the PRE2 for the Cisco 10000 series router.
12.2(31)SB2	This command was introduced on the PRE3 for the Cisco 10000 series router.

Usage Guidelines

Cisco 10000 Series Router (PRE2)

Because memory is shared between TurboACLs and MiniACLs, they can interfere with each other's capacities. The Mini-ACL is automatically set up with space for 8191 Mini-ACLs at router start. If more than 8191 Mini-ACLs are created, another block of MiniACLs (4096) is allocated. This process is repeated as necessary until the router is out of External Column Memory (XCM) in any one bank that the Mini-ACLs need.

Cisco 10000 Series router (PRE3)

The PRE3 implements only TCAM ACLs. Turbo-ACLs and Mini-ACLs are not supported.

Examples

The sample output from the **show pxf cpu access-lists security** command (see Sample Output) is based on the configuration of the access control list (ACL) called test_list (see ACL Configuration). The sample output is divided into several sections with a description of the type of information displayed in each.

ACL Configuration

```
Router# show pxf cpu access-lists test_list
Extended IP access list test_list (Compiled)
    10 permit ip any host 10.1.1.1
    20 permit ip any host 10.1.1.2
    30 permit ip any host 10.1.1.3
    40 permit ip any host 10.1.1.4
    50 permit ip any host 10.1.1.5
    60 permit ip any host 10.1.1.6
    70 permit ip any host 10.1.1.7
    80 permit ip any host 10.1.1.8
    90 permit ip any host 10.1.1.9
    100 permit ip any host 10.1.1.11
    110 permit ip any host 10.1.1.12
```

Sample Output

The following sample output describes the information displayed in the first section of the command output from the **show pxf cpu access-lists security** command:

```
Router# show pxf cpu access-lists security
PXF Security ACL statistics:
ACL            State      Tables  Entries  Config  Fragment  Redundant  Memory ACL_index
 1            Operational   1        -        -        -         -         0Kb     1
sl_def_acl    Operational   2        -        -        -         -         0Kb     2
test          Operational   3        -        -        -         -         0Kb     3
test_list     Operational   1        12       11       0         0         7Kb     1
```

The table below describes the significant fields shown in the display.

Table 259: show pxf cpu access-lists security Field Descriptions

Field	Description
ACL	Identifies the ACL by name or number.
State	Displays the current state of the ACL: • Copying--ACL is in the process of being created or compiled. • Operational--ACL is active and filtering packets. • Out of acl private mem--ACL has run out of the private memory that was allocated exclusively to it. • Out of shared mem--ACL has run out of the memory that it shares with other ACLs. • Unknown Failure--ACL has failed because of an uncategorized reason. • Unneeded--ACL was allocated but is not currently in use.
Tables	An indicator of whether the ACL has been split into more than one PXF pass. The first three ACLs in the output are MiniACLs, and have the ACL_index duplicated in the Tables column.
Entries	The count of ACL rules as seen by the Turbo compiler. This is the sum of the Config, Fragment, and Redundant columns plus 1.
Config	The count of rules for this ACL.
Fragment	The count of extra rules added to handle fragment handling, where Layer 4 information is needed but not available in a packet fragment.
Redundant	The count of rules that are not needed because they are covered by earlier rules.
Memory	The amount of PXF XCM in use for the ACL.
ACL_index	The index of the ACL in XCM.

The following sample output describes the information displayed in the next section of the command output from the **show pxf cpu access-lists security** command:

```
First level lookup tables:
Block      Use              Rows       Columns   Memory used
  0   TOS/Protocol            1/128     1/32      16384
  1   IP Source (MS)          1/128     1/32      16384
  2   IP Source (LS)          1/128     1/32      16384
  3   IP Dest (MS)            2/128     1/32      16384
  4   IP Dest (LS)           12/128     1/32      16384
  5   TCP/UDP Src Port        1/128     1/32      16384
  6   TCP/UDP Dest Port       1/128     1/32      16384
  7   TCP Flags/Fragment      1/128     1/32      16384
```

The table below describes the significant fields shown in the display.

Table 260: show pxf cpu access-lists security Field Descriptions

Field	Description
Block	Indicates the block number.
Use	Describes the IP packet field that is being matched.
Rows	An indication of where the largest variety of values are in use in the ACLs that are being applied. In the output, 12/128 means that there are 12 different values of significance in the field. If there are other rules added and the value exceeds 128, more memory will be needed to accommodate the new rules.
Columns	An indication of the number of TurboACLs in PXF memory. In the output, 1/32 means there is only one TurboACL in PXF memory. If there are more than 31 added, another chunk of memory is needed to accommodate the new ACLs.
Memory used	Displays the total amount of memory used for this particular lookup table.

The following sample output describes the information displayed in the next section of the command output from the **show pxf cpu access-lists security** command. There are 16 banks of XCM in each PXF column. This output section shows the usage level of each bank.

```
Banknum   Heapsize   Freesize  %Free
   0       4718592    4702208    99
   1       8126464    6012928    73
   2       8388608    6290432    74
   3       8388608    6290432    74
   4       5898240    5881856    99
   5       8126464    6012928    73
   6       8388608    6290432    74
   7       8126464    6012928    73
   8       4456448    4440064    99
   9       8126464    6012928    73
```

The table below describes the significant fields shown in the display.

Table 261: show pxf cpu access-lists security Field Descriptions

Field	Description
Banknum	The block of memory used for this particular lookup table.
Heapsize	The total amount of memory, in bytes, allocated for this block.
Freesize	The amount of memory, in bytes, that is currently available for use by this block of memory.
%Free	The percentage of memory that is free and available for use for this block of memory. When the %Free drops to 0, the router cannot hold any more ACLs in PXF memory, and any new ACL will not pass traffic.

This section of the sample command output indicates the memory usage of the MiniACLs in the router. All of the rows state about the same thing. To determine the actual number of MiniACLs in play, divide the memory used in any of blocks 1 to 10 by 256, or blocks 11 to 14 by 16.

```
MiniACL XCM Tables:
```

```
Block   Use               Memory Used   %Free
  0   IP Src 1              768        99
  1   IP Src 2              768        99
  2   IP Src 3              768        99
  3   IP Src 4              768        99
  4   IP Dest 1             768        99
  5   IP Dest 2             768        99
  6   IP Dest 3             768        99
  7   IP Dest 4             768        99
  8   ToS                   768        99
  9   Protocol              768        99
  10  TCP Flags/Fragment    768        99
  11  Source Port 1          48        99
  12  Source Port 2          48        99
  13  Destination Port 2     48        99
  14  Destination Port 2     48        99
```

The following describes the information displayed in the last section of the sample output from the **show pxf cpu access-lists security** command:

```
Available MiniACL count = 8191
Usable ranges(inclusive):
1->8191
```

The table below describes the significant fields shown in the display.

Table 262: show pxf cpu access-lists security Field Descriptions

Field	Description
Available MiniACL	The number of ACLs currently available for allocation in XCM.
Usable ranges	The ACL indexes that will be assigned to MiniACLs.

PRE2 and PRE3 Security ACLs Examples (Cisco 10000 Series Router)

This section compares the output from the **show pxf cpu access-lists security** command when issued on the PRE2 and PRE3.

For the PRE2, the following sample output displays VMR (value, plus a mask and result) data for the ACL named ICMP_IGMP_MATCH:

```
Router# show pxf cpu access-lists security tcam ICMP_IGMP_MATCH detail

-------------------------------------------------------------
VMR Format - handle: 524607B4
Format has 5 fields, refcount = 1
Field: Format, FIXED, start_bit = 69, end_bit = 71
Field: ACL index, FIXED, start_bit = 54, end_bit = 68
Field: Flags, FIXED, start_bit = 43, end_bit = 53
Field: L4 proto, FIXED CNV, start_bit = 16, end_bit = 23
Field: L4 source port, FIXED CNV, start_bit = 0, end_bit = 15 Total bits = 53, format = 72
 GMR used: 5 Col 2 LKBP Vector: 544
-------------------------------------------------------------
VMRs
------ VMR 0 ------
V: 001B0000 0000010B 00
M: FFFFC000 0000FFFF FF
R: 00010001
Format: 00000000/00000007
ACL index: 0000006C/00007FFF
```

```
L4 source port: 00000B00/0000FFFF
L4 proto: 00000001/000000FF
Flags: 00000000/00000000
------ VMR 1 ------
V: 001B0000 00000103 01
M: FFFFC000 0000FFFF FF
R: 00010002
Format: 00000000/00000007
ACL index: 0000006C/00007FFF
L4 source port: 00000301/0000FFFF
L4 proto: 00000001/000000FF
Flags: 00000000/00000000
------ VMR 2 ------
V: 001B0000 00000213 00
M: FFFFC000 0000FFFF 00
R: 00010003
Format: 00000000/00000007
ACL index: 0000006C/00007FFF
L4 source port: 00001300/0000FF00
L4 proto: 00000002/000000FF
Flags: 00000000/00000000
------ VMR 3 ------
V: 001B0000 00000214 00
M: FFFFC000 0000FFFF 00
R: 00010004
Format: 00000000/00000007
ACL index: 0000006C/00007FFF
L4 source port: 00001400/0000FF00
L4 proto: 00000002/000000FF
Flags: 00000000/00000000
```

For the PRE3, the following sample output displays for the **show pxf cpu access-lists security** command. Notice that the output does not include the columns shown above that are relevant to only the PRE2 and the output no longer displays first-level lookup tables.

```
Router# show pxf cpu access-lists security

PXF Security ACL statistics:
 ACL                                     State          ACL_index
STANDARD_MATCH_PERMIT                   Operational          116
SRC_IP_MATCH144                         Operational          102
DST_IP_MATCH                            Operational          113
DST_IP_MATCH144                         Operational          112
PROTOCOL_MATCH                          Operational          104
PROTOCOL_MATCH144                       Operational          103
FRAG_MATCH                              Operational          109
PRECEDENCE_TOS_MATCH                    Operational          106
PRECEDENCE_TOS_MATCH144                 Operational          105
```

Related Commands

Command	Description
show pxf cpu statistics	Displays PXF CPU statistics.
show pxf statistics	Displays a chassis-wide summary of PXF statistics.

show pxf cpu iedge

To display Parallel eXpress Forwarding (PXF) policy and template information, use the **show pxf cpu iedge**command in privileged EXEC mode.

show pxf cpu iedge[{ **detail** | **policy** *policy-name* | **template**}]

Syntax Description

detail	(Optional) Displays detailed information about policies and templates.
policy *policy-name*	(Optional) Displays summary policy information.
template	(Optional) Displays summary template information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2S	This command was introduced.

Examples

The following example shows PXF template information. The fields shown in the display are self-explanatory.

```
Router# show pxf cpu iedge template
Super ACL name                     OrigCRC   Class Count    CalcCRC
1sacl_2                           4EA94046   2             00000000
if_info 71BA3F20
```

Related Commands

Command	Description
show pxf statistics	Displays a summary of PXF statistics.

show pxf cpu qos

To display Parallel eXpress Forwarding (PXF) External Column Memory (XCM) contents related to a particular policy, use the **show pxf cpu qos** command in privileged EXEC mode.

show pxf cpu qos [{**policy-map** *policy-name* | **vcci-maps**}]

Cisco 10000 Series Router
show pxf cpu qos [{*vcci* | **classifiers** | **flex-sum** | **policy-map** *policy-name* | **vcci-maps**}]

Syntax Description

vcci	(Optional) Virtual Channel Circuit Identifier (VCCI). Information about this specified VCCI will be displayed.
classifiers	(Optional) Displays information about the criteria used to classify traffic.
flex-sum	(Optional) Displays summary information describing the amount of memory allocated in the PXF engine for use by the flexible key construction microcode. **Note** This option is only available on the Cisco 10000 series router for the PRE3.
policy-map *policy-name*	(Optional) Displays per-policy map information.
vcci-maps	(Optional) Displays VCCI map values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2S	This command was introduced.
12.3(7)XI1	This command was introduced on the Cisco 10000 series router for the PRE2.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(31)SB2	This command was introduced on the PRE3 for the Cisco 10000 series router.

Usage Guidelines

This command is useful in verifying the presence of a policy on interfaces and indexes programmed in the PXF.

Examples

The following example shows XCM contents related to a policy called police_test, which is defined as follows:

```
policy-map police_test
 class high-priority
 priority
 class low-priority
  set atm-clp
 class class-default
```

```
    queue-limit 512
Router# show pxf cpu qos police_test
Output Policymap: police_test
 Vcci: A05  Flags: 4  Policymap_index: 6  Policymap_data_index: 12
 OUT AT1/0/0.111 (0x71764660) ref_count 1
Output Action Table Contents for vcci 0xA05 - Policymap index: 6
 class-name: high-priority  class_index: 0  action_flags: 0x00
  srp_class_id: 0x01  prec/dscp: 0x00  cos: 0
  discard_class: 0x00  exp_value: 0
class-name: low-priority  class_index: 1  action_flags: 0x10
  srp_class_id: 0x00  prec/dscp: 0x00  cos: 0
  discard_class: 0x00  exp_value: 0
class-name: class-default  class_index: 2  action_flags: 0x00
  srp_class_id: 0x00  prec/dscp: 0x00  cos: 0
  discard_class: 0x00  exp_value: 0
```

Related Commands

Command	Description
show pxf cpu statistics qos	Displays match statistics for a service policy on an interface.

show pxf dma

To display the current state of direct memory access (DMA) buffers, error counters, and registers on the Parallel eXpress Forwarding (PXF), use the **show pxf dma**command in privileged EXEC mode.

show pxf dma [{**buffers** | **counters** | **reassembly** | **registers**}]

Cisco 10000 Series Router (PRE3 only)

show pxf dma [{**buffers** | **counters** | **reassembly** | **registers**}][{**brief** | **config** | **errors** | **status**}]

Syntax Description

buffers	(Optional) Displays PXF DMA buffers information.
counters	(Optional) Displays packet and error counters for the PXF DMA engine.
reassembly	(Optional) Displays PXF reassembly table usage information.
registers	(Optional) Displays PXF DMA registers information.
brief	(Optional) Displays PXF DMA information, including the initialization state of each block in the PXF API and any errors that occurred. **Note** This option is available on the PRE3 only.
config	(Optional) Displays a configuration summary of the registers in each of the PXF DMA blocks. **Note** This option is available on the PRE3 only.
errors	(Optional) Displays the errors that occurred in each of the PXF DMA blocks. **Note** This option is available on the PRE3 only.
status	(Optional) Displays the initialization state of each PXF DMA block. In normal operation, all blocks display the enabled state. **Note** This option is available on the PRE3 only.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2S	This command was introduced.
12.3(7)XI	This command was integrated into Cisco IOS Release 12.3(7)XI and implemented on the Cisco 10000 series router for the PRE2.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2 and implemented on the Cisco 10000 series router for the PRE3.

Examples

The following example shows PXF DMA buffers information:

```
Router# show pxf dma buffers
PXF To-RP DMA Ring Descriptors & Buffers:
     Descriptor       Buffer        Buffer      Descriptor
     Address          Address       Length(b)   Flags
0    0x0CA06340       0x0AC097C0      512       0x0002
1    0x0CA06350       0x0AC088C0      512       0x0002
2    0x0CA06360       0x0AC07C40      512       0x0002
3    0x0CA06370       0x0AC0B5C0      512       0x0002
4    0x0CA06380       0x0AC0CC40      512       0x0002
5    0x0CA06390       0x0AC08640      512       0x0002
6    0x0CA063A0       0x0AC0C240      512       0x0002
7    0x0CA063B0       0x0AC08B40      512       0x0002
8    0x0CA063C0       0x0AC0AE40      512       0x0002
9    0x0CA063D0       0x0AC0BAC0      512       0x0002
10   0x0CA063E0       0x0AC0C9C0      512       0x0002
11   0x0CA063F0       0x0AC09CC0      512       0x0002
12   0x0CA06400       0x0AC0C740      512       0x0002
13   0x0CA06410       0x0AC0A6C0      512       0x0002
14   0x0CA06420       0x0AC0B0C0      512       0x0002
15   0x0CA06430       0x0AC09040      512       0x0002
16   0x0CA06440       0x0AC0A440      512       0x0002
17   0x0CA06450       0x0AC065C0      512       0x0002
18   0x0CA06460       0x0AC06FC0      512       0x0002
19   0x0CA06470       0x0AC06340      512       0x0002
20   0x0CA06480       0x0AC07240      512       0x0002
21   0x0CA06490       0x0AC092C0      512       0x0002
22   0x0CA064A0       0x0AC0D140      512       0x0002
23   0x0CA064B0       0x0AC0C4C0      512       0x0002
24   0x0CA064C0       0x0AC07740      512       0x0002
25   0x0CA064D0       0x0AC09540      512       0x0002
26   0x0CA064E0       0x0AC0A940      512       0x0002
27   0x0CA064F0       0x0AC06840      512       0x0002
28   0x0CA06500       0x0AC08140      512       0x0002
29   0x0CA06510       0x0AC06D40      512       0x0002
30   0x0CA06520       0x0AC07EC0      512       0x0002
31   0x0CA06530       0x0AC0ABC0      512       0x0003
PXF From-RP DMA Ring Descriptors & Buffers:
     Descriptor       Buffer        Buffer      Descriptor    Context
     Address          Address       Length(b)   Flags         Bit
0    0x0CA06580       0x00000000        0       0x0000        Not set
1    0x0CA06590       0x00000000        0       0x0000        Not set
2    0x0CA065A0       0x00000000        0       0x0000        Not set
3    0x0CA065B0       0x00000000        0       0x0000        Not set
4    0x0CA065C0       0x00000000        0       0x0000        Not set
5    0x0CA065D0       0x00000000        0       0x0000        Not set
6    0x0CA065E0       0x00000000        0       0x0000        Not set
7    0x0CA065F0       0x00000000        0       0x0000        Not set
8    0x0CA06600       0x00000000        0       0x0000        Not set
9    0x0CA06610       0x00000000        0       0x0000        Not set
10   0x0CA06620       0x00000000        0       0x0000        Not set
11   0x0CA06630       0x00000000        0       0x0000        Not set
12   0x0CA06640       0x00000000        0       0x0000        Not set
13   0x0CA06650       0x00000000        0       0x0000        Not set
14   0x0CA06660       0x00000000        0       0x0000        Not set
15   0x0CA06670       0x00000000        0       0x0001        Not set
```

The table below describes the fields shown in the display.

Table 263: show pxf dma Field Descriptions

Field	Description
Descriptor Address	Memory address pointing to the descriptor for this buffer.
Buffer Address	Address of this buffer in memory.
Buffer Length	Length, in bytes, of this particular buffer.
Descriptor Flags	Internal flags identifying this buffer's use and status.
Context Bit	State of the context bit which is set when the buffer is currently in use by a context (the basic unit of packet processing).

Related Commands

Command	Description
clear pxf	Clears PXF counters and statistics.
show pxf cpu	Displays PXF CPU statistics.
show pxf microcode	Displays the microcode version running on the PXF.

show pxf max-logical-interfaces

To display the configuration for the maximum number of classes permitted per QoS policy in PXF and the maximum number of PXF logical interfaces allowed on the router, use the **showpxfmax-logical-interfaces** command in privileged EXEC mode.

show pxf max-logical-interfaces

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(20)S5	This command was introduced.

Usage Guidelines

The **showpxfmax-logical-interfaces** command is used to verify if the **pxfmax-logical-interfaces** configuration change was accepted by the router. The output from this command provides the settings for the maximum number of classes permitted per QoS policy in PXF and the number of PXF logical interfaces as set in both the running configuration file and the startup configuration file. The settings listed in the startup configuration file are the current settings on the router; the settings listed in the running configuration will be the settings on the router when the router is reloaded.

Examples

In the following example, the **pxfmax-logical-interfaces16k** command has been entered to change the setting from the previous setting of 4k. The router, however, has not been rebooted with the changes saved to the running configuration.

```
Router# show pxf max-logical-interfaces
Running configuration:
    PXF Max classes per interface: 23
    Max PXF interfaces:            16K
Startup configuration:
    PXF Max classes per interface: 64
    Max PXF interfaces:            4K
```

Related Commands

Command	Description
pxf max-logical-interfaces	Configures the maximum number of PXF logical interfaces permitted on the router.

show qm-sp port-data

To display information about the QoS-manager switch processor, use the **showqm-spport-data** command in privileged EXEC mode.

show **qm-sp** **port-data** *mod* *port*

Syntax Description

mod port	Module and port number; see the “Usage Guidelines” section for valid values.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported by the supervisor engine only and can be entered only from theCisco 7600 series routers console (see the **remotelogin** command).

The *modport* arguments designate the module and port number. Valid values depend on the chassis and module that are used. For example, if you have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

Enter the **showqm-spport-data**command to verify the values that are programmed in the hardware.

Examples

This example shows how to display information about the QoS manager:

```
Router# show qm-sp port-data 1 2
-----------------------------------------------------------------------------
* Type: Tx[1p2q2t] Rx[1p1q4t]  [0] Pinnacle
* Per-Port: [Untrusted] Default COS[0] force[0] [VLAN based]
-----------------------------------------------------------------------------
* COSMAP(C[Q/T]) TX: 0[1/1] 1[1/1] 2[1/2] 3[1/2] 4[2/1] 5[3/1] 6[2/1] 7[2/2]
                 RX: 0[1/1] 1[1/1] 2[1/2] 3[1/2] 4[1/3] 5[2/1] 6[1/3] 7[1/4]
-----------------------------------------------------------------------------
* WRR bandwidth:        [7168 18432]
* TX queue limit(size): [311296 65536 65536]
* WRED queue[1]:        failed (0x82)
       queue[2]:        failed (0x82)
-----------------------------------------------------------------------------
* TX drop thr queue[1]: type[2 QOS_SCP_2_THR] dropThr[311104 311104]
              queue[2]: type[2 QOS_SCP_2_THR] dropThr[61504 61504]
* RX drop threshold:    type[4 QOS_SCP_4_THR] dropThr[62259 62259 62259 62259]
* RXOvr drop threshold: type[0 UNSUPPORTED] dropThr[16843009 131589 61504 61504]
* TXOvr drop threshold: type[0 UNSUPPORTED] dropThr[67174656 260 16843009 131589]
Switch-sp#
```

Related Commands

Command	Description
rcv-queue queue-limit	Sets the size ratio between the strict-priority and standard receive queues.
remote login	Accesses the Cisco 7600 series routers console or a specific module.
wrr-queue bandwidth	Allocates the bandwidth between the standard transmit queues.
wrr-queue queue-limit	Sets the transmit-queue size ratio on an interface.
wrr-queue threshold	Configures the drop-threshold percentages for the standard receive and transmit queues on 1q4t and 2q2t interfaces.

show rbscp

To display state and statistical information about Rate Based Satellite Control Protocol (RBSCP) tunnels, use the **showrbscp** command in user EXEC or privileged EXEC mode.

show rbscp {**all** | **inbound** | **state** | **statistics**} [**tunnel** *tunnel-number*]

Syntax Description

all	Displays both RBSCP state and RBSCP statistical information.
inbound	Displays all the RBSCP inbound queue dump information.
state	Displays the RBSCP state information.
statistics	Displays RBSCP statistical information.
tunnel *tunnel-number*	(Optional) Displays the RBSCP information for a specific tunnel interface in the range from 0 to 2147483647. If a tunnel interface is not specified, information for all RBSCP tunnels is displayed.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.4(22)T	This command was modified. The **inbound** keyword was added.
Cisco IOS 2.1 XE	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The output of this command is useful when you need to configure and monitor RBSCP tunnels. The output shows various state and statistical information about RBSCP tunnels.

Examples

The following is sample output from the **showrbscpall**command:

```
Router# show rbscp all
Tunnel0 is up, line protocol is up
RBSCP operational state:  IS OPENING
RBSCP operating mode: (264h) ack_split window_stuffing inorder SCTP_report
  window step: 1
  drop scale : 0
  ACK split size: 4
  input drop scale: 2
  initial TSN: 1h
  fuzz factor: 0
  next TSN: 1h
  next sequence: 1h
  current outstanding: 0
  max out per RTT: 68750
  packets since SACK: 0
  cumulative ack: 0h
  TSN at SACK: 1h
  last cumulative ack: 0h
```

```
  last delivered TSN: 0h
  next FWDTSN corr: 6h
  RTO: 704 ms
  RTT: 550 ms     srtt_sa: 0      srtt_sv: 4
  sentQ: num packets: 0, num bytes: 0
  tmitQ: num packets: 0, num bytes: 0
RBSCP protocol statistics:
  Init FWD-TSNs sent 0, received 0
  TUNNEL-UPs sent 0, received 0
  CLOSEDs sent 0, received 0
  TSNs sent 0, resent 0, lost by sender 0
  TSNs received 0 (duplicates 0)
  FWD-TSNs sent 63 (heartbeats 0)
  FWD-TSNs received 0 (ignored 0)
  FWD-TSNs caused 0 packet drops, 0 whole window drops
  SACKs sent 0, received 0 (ignored 0)
  Recovered with RTX 0
  Received with delay 0
  Most released at once 0
  Failed sends into the: tunnel 1, network 0
  Dropped due to: excess delay 0, tmit queue full 0
  Max on any queue: num packets: 0, num bytes: 0
  Max outstanding: 0
```

The table below describes the significant fields shown in the display.

Table 264: show rbscp all Field Descriptions

Field	Description
Tunnel*n* is {up | down}	Interface is currently active (up) or inactive (down).
line protocol is {up | down | administratively down}	Shows line protocol up if a valid route is available to the tunnel destination. Shows line protocol down if no route is available or if the route would be recursive.
RBSCP operational state	Indicates the current RBSCP state.
RBSCP operating mode	Indicates the RBSCP operating mode.
window step	Step size for the window scale.
drop scale	Scale factor for the number of bytes that can be queued before packets are dropped on the output side.
Ack split size	Number of TCP acknowledgements to send for every ack received.
input drop scale	Scale factor for the number of bytes that can be queued before packets are dropped on the input side.
initial TSN	Transport Sequence Number (TSN) of the first outgoing RBSCP/IP packet sent to a peer. RBSCP uses sequence numbers to ensure a reliable service. Peers will send the TSN back in the acknowledgment packet.
fuzz factor	Value added to the RBSCP delay clock to pad the delay when large round-trip time (RTT) fluctuations occur.
next TSN	TSN of the next outgoing RBSCP/IP packet.

Field	Description
next sequence	Next sequence number to use, in hexadecimal format.
current outstanding	Current number of bytes that are in transit or are unacknowledged.
max out per RTT	Maximum number of bytes allowed to be sent out per RTT.
packets sent since SACK	Number of packets sent since an RBSCP Selective Acknowledgement (SACK).
cumulative ack	Cumulative acknowledgement point that is the highest in sequence TSN that was received from a peer.
TSN at SACK	Value of highest TSN for the last SACK that was received from a peer.
last cumulative ack	Last cumulative acknowledgement point that was received from the peer.
last delivered TSN	Last TSN received that was subsequently delivered to an upper level protocol.
next FWDTSN corr	Next FWD_TSN correlation entry to use.
RTO	Retransmission timeout, in milliseconds.
RTT	Round-trip time estimate, in milliseconds.
srtt_sa	Smoothed round-trip time average.
srtt_sv	Smoothed round-trip time variance.
sentQ	Number of packets and bytes sent but not yet acknowledged.
tmitQ	Number of packets and bytes ready to be sent.
Init FWD-TSNs	Number of TSNs sent and received for initializing the RBSCP tunnel.
TUNNEL-UPs	Number of TUNNEL_UP messages sent and received.
CLOSEDs	Number of CLOSED messages sent and received.
heartbeats	Heartbeats are equivalent to keepalive messages.
Recovered with RTX	Number of packets recovered using a retransmitted message.
Received with delay	Number of packets that included a delay value.
Most released at once	Maximum burst of packets sent in one interval.
Failed sends	Number of packets that were sent but failed because of an internal error, such as no route or the underlying interface is down.

The following is sample output from the **showrbscpstate**command:

```
Router# show rbscp state
```

```
Tunnel0 is up, line protocol is up
RBSCP operational state:  IS OPENING
RBSCP operating mode: (264h) ack_split window_stuffing inorder SCTP_report
  window step: 1
  drop scale : 0
  ACK split size: 4
  input drop scale: 2
  initial TSN: 1h
  fuzz factor: 0
  next TSN: 1h
  next sequence: 1h
  current outstanding: 0
  max out per RTT: 68750
  packets since SACK: 0
  cumulative ack: 0h
  TSN at SACK: 1h
  last cumulative ack: 0h
  last delivered TSN: 0h
  next FWDTSN corr: 0h
  RTO: 704 ms
  RTT: 550 ms     srtt_sa: 0      srtt_sv: 4
  sentQ: num packets: 0, num bytes: 0
  tmitQ: num packets: 0, num bytes: 0
```

The following is sample output from the **showrbscpstatistics**command:

```
Router# show rbscp statistics tunnel 0
Tunnel0 is up, line protocol is up
RBSCP protocol statistics:
  Init FWD-TSNs sent 0, received 0
  TUNNEL-UPs sent 0, received 0
  CLOSEDs sent 0, received 0
  TSNs sent 0, resent 0, lost by sender 0
  TSNs received 0 (duplicates 0)
  FWD-TSNs sent 136 (heartbeats 0)
  FWD-TSNs received 0 (ignored 0)
  FWD-TSNs caused 0 packet drops, 0 whole window drops
  SACKs sent 0, received 0 (ignored 0)
  Recovered with RTX 0
  Received with delay 0
  Most released at once 0
  Failed sends into the: tunnel 1, network 0
  Dropped due to: excess delay 0, tmit queue full 0
  Max on any queue: num packets: 0, num bytes: 0
  Max outstanding: 0
```

Related Commands

Command	Description
clear rbscp	Resets and restarts RBSCP tunnels.

show redundancy

To display current or historical status and related information on planned or logged handovers, use the **show redundancy** command in user EXEC or privileged EXEC mode.

Privileged EXEC Mode
show redundancy [{**clients** | **counters** | **debug-log** | **handover** | **history** | **inter-device** | **states** | **switchover** | **switchover history**}]

User EXEC Mode
show redundancy {**clients** | **counters** | **history** | **states** | **switchover**}

Syntax Description

clients	(Optional) Displays the redundancy-aware client-application list.
counters	(Optional) Displays redundancy-related operational measurements.
debug-log	(Optional) Displays up to 256 redundancy-related debug entries.
handover	(Optional) Displays details of any pending scheduled handover.
history	(Optional) Displays past status and related information about logged handovers. This is the only keyword supported on the Cisco AS5800.
inter-device	(Optional) Displays redundancy interdevice operational state and statistics.
states	(Optional) Displays redundancy-related states: disabled, initialization, standby, active (various substates for the latter two), client ID and name, length of time since the client was sent the progression, and event history for the progression that was sent to the client.
switchover	(Optional) Displays the switchover counts, the uptime since active, and the total system uptime.
switchover history	(Optional) Displays redundancy switchover history.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
11.3(6)AA	This command was introduced in privileged EXEC mode.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5800 and Cisco AS5850 is not included in this release.
12.2(8)MC2	This command was modified. This command was made available in user EXEC mode.
12.2(11)T	The privileged EXEC mode form of this command was implemented on the Cisco AS5800 and Cisco AS5850.

Release	Modification
12.2(14)SX	The user EXEC mode form of this command was implemented on the Supervisor Engine 720.
12.2(18)S	This command was implemented on Cisco 7304 routers running Cisco IOS Release 12.2S.
12.2(20)S	The **states**, **counters**, **clients**, **history**, and **switchover history** keywords were added.
12.2(17d)SXB	Support for the user EXEC mode form of this command was extended to the Supervisor Engine 2.
12.3(8)T	The **inter-device** keyword was added to the privileged EXEC form of the command.
12.3(11)T	The user EXEC form of this command was integrated into Cisco IOS Release 12.3(11)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SGA	This command was integrated into Cisco IOS Release 12.2(31)SGA.
12.2(33)SRB	The **clients** keyword was enhanced to provide information about the status of each client.
12.2(33)SRB1	ISSU is supported on the Cisco 7600 series routers in Cisco IOS Release 12.2(33)SRB1.
12.2(31)SXH	This command was integrated into Cisco IOS Release 12.2(31)SXH.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 3.1S	More information regarding the **states** keyword was added.

Usage Guidelines

Cisco AS5800

Use this command from the router-shelf console to determine when failover is enabled. Use this command with the **history** keyword to log failover events.

Cisco AS5850

To use this command, the router must have two route-switch-controller (RSC) cards installed and must be connected to one of them.

Examples

The following example shows how to display information about the RF client:

```
Router# show redundancy clients
 clientID = 0       clientSeq = 0         RF_INTERNAL_MSG
 clientID = 25      clientSeq = 130       CHKPT RF
 clientID = 5026    clientSeq = 130       CHKPT RF
 clientID = 5029    clientSeq = 135       Redundancy Mode RF
```

```
 clientID = 5006    clientSeq = 170      RFS client
 clientID = 6       clientSeq = 180      Const OIR Client
 clientID = 7       clientSeq = 190      PF Client
 clientID = 5008    clientSeq = 190      PF Client
 clientID = 28      clientSeq = 330      Const Startup Config
 clientID = 29      clientSeq = 340      Const IDPROM Client
 clientID = 65000   clientSeq = 65000    RF_LAST_CLIENT
```

The output displays the following information:

- clientID displays the client's ID number.
- clientSeq displays the client's notification sequence number.
- Current RF state.

The following example shows how to display information about the RF counters:

```
Router# show redundancy counters
Redundancy Facility OMs
               comm link up = 0
        comm link down down = 0
          invalid client tx = 0
          null tx by client = 0
                tx failures = 0
      tx msg length invalid = 0
      client not rxing msgs = 0
 rx peer msg routing errors = 0
           null peer msg rx = 0
        errored peer msg rx = 0
                 buffers tx = 0
     tx buffers unavailable = 0
                 buffers rx = 0
      buffer release errors = 0
 duplicate client registers = 0
  failed to register client = 0
       Invalid client syncs = 0
```

The following example shows information about the RF history:

```
Router# show redundancy history
00:00:00 client added: RF_INTERNAL_MSG(0) seq=0
00:00:00 client added: RF_LAST_CLIENT(65000) seq=65000
00:00:02 client added: Const Startup Config Sync Clien(28) seq=330
00:00:02 client added: CHKPT RF(25) seq=130
00:00:02 client added: PF Client(7) seq=190
00:00:02 client added: Const OIR Client(6) seq=180
00:00:02 client added: Const IDPROM Client(29) seq=340
00:00:02 *my state = INITIALIZATION(2) *peer state = DISABLED(1)
00:00:02 RF_PROG_INITIALIZATION(100) RF_INTERNAL_MSG(0) op=0 rc=11
00:00:02 RF_PROG_INITIALIZATION(100) CHKPT RF(25) op=0 rc=11
00:00:02 RF_PROG_INITIALIZATION(100) Const OIR Client(6) op=0 rc=11
00:00:02 RF_PROG_INITIALIZATION(100) PF Client(7) op=0 rc=11
```

The following example shows information about the RF state:

```
Router# show redundancy states
       my state = 13 -ACTIVE
     peer state = 1  -DISABLED
           Mode = Simplex
           Unit = Primary
        Unit ID = 1
```

```
Redundancy Mode (Operational) = Route Processor Redundancy
Redundancy Mode (Configured)  = Route Processor Redundancy
     Split Mode = Disabled
   Manual Swact = Disabled  Reason: Simplex mode
 Communications = Down      Reason: Simplex mode
   client count = 11
 client_notification_TMR = 30000 milliseconds
          keep_alive TMR = 4000 milliseconds
        keep_alive count = 0
    keep_alive threshold = 7
           RF debug mask = 0x0
```

If you enter the **show redundancy states** command with stateful switchover (SSO) configured, the Redundancy Mode (Operational) and the Redundancy Mode (Configured) fields display stateful switchover.

The following example shows how to display the switchover counts, the uptime since active, and the total system uptime:

```
Router> show redundancy switchover
Switchovers this system has experienced          : 1
Uptime since this supervisor switched to active  : 1 minute
Total system uptime from reload                  : 2 hours, 47 minutes
```

Example: Setting the terminal length for the Cisco ASR 1006

The following example shows how to set the terminal length value to pause the multiple-screen output:

```
Router# terminal length 5
Router# show redundancy states
my state = 13 -ACTIVE
     peer state = 8  -STANDBY HOT
           Mode = Duplex
           Unit = Primary
        Unit ID = 48
```

Example: Cisco AS5850

The following is sample output from the **show redundancy handover** and **show redundancy states** commands on the Cisco AS5850:

```
Router# show redundancy handover

No busyout period specified
Handover pending at 23:00:00 PDT Wed May 9 2001
Router# show redundancy states

my state = 14 -ACTIVE_EXTRALOAD
peer state = 4 -STANDBY COLD
Mode = Duplex
Unit = Preferred Primary
Unit ID = 6
Redundancy Mode = Handover-split: If one RSC fails, the peer RSC will take over the
feature boards
Maintenance Mode = Disabled
Manual Swact = Disabled Reason: Progression in progress
```

```
Communications = Up
client count = 3
client_notification_TMR = 30000 milliseconds
keep_alive TMR = 4000 milliseconds
keep_alive count = 1
keep_alive threshold = 7
RF debug mask = 0x0
```

Example: Cisco AS5800

The following is sample output from the **show redundancy** command on the Cisco AS5800:

```
Router# show redundancy
DSC in slot 12:
Hub is in 'active' state.
Clock is in 'active' state.
DSC in slot 13:
Hub is in 'backup' state.
Clock is in 'backup' state.
```

Example: Cisco AS5800 with History

The following is sample output from the **show redundancy history** command on the Cisco AS5800:

```
Router# show redundancy history
DSC Redundancy Status Change History:
981130 18:56 Slot 12 DSC: Hub, becoming active - RS instruction
981130 19:03 Slot 12 DSC: Hub, becoming active - D13 order
```

Example: Cisco AS5800 Router Shelves as Failover Pair

The following is sample output from two Cisco AS5800 router shelves configured as a failover pair. The active router shelf is initially RouterA. The **show redundancy history** and **show redundancy** commands have been issued. The **show redundancy** command shows that failover is enabled, shows the configured group number, and shows that this router shelf is the active one of the pair. Compare this output with that from the backup router shelf (RouterB) that follows.

Note When RouterA is reloaded, thereby forcing a failover, new entries are shown on RouterB when the**show redundancy history** command is issued after failover has occurred.

Log from the First Router (RouterA)

```
RouterA# show redundancy history
DSC Redundancy Status Change History:
010215 18:17 Slot -1 DSC:Failover configured -> ACTIVE role by default.
010215 18:18 Slot -1 DSC:Failover -> BACKUP role.
010215 18:18 Slot 12 DSC:Failover -> ACTIVE role.
010215 18:18 Slot 12 DSC:Hub, becoming active - arb timeout
RouterA# show redundancy
```

```
failover mode enabled, failover group = 32
Currently ACTIVE role.
DSC in slot 12:
Hub is in 'active' state.
Clock is in 'active' state.
No connection to slot 13
RouterA# reload
Proceed with reload? [confirm] y
*Feb 15 20:19:11.059:%SYS-5-RELOAD:Reload requested
System Bootstrap, Version xxx
Copyright xxx by cisco Systems, Inc.
C7200 processor with 131072 Kbytes of main memory
```

Log from the Second Router (RouterB)

```
RouterB# show redundancy
failover mode enabled, failover group = 32
Currently BACKUP role.
No connection to slot 12
DSC in slot 13:
Hub is in 'backup' state.
Clock is in 'backup' state.
*Feb 16 03:24:53.931:%DSC_REDUNDANCY-3-BICLINK:Switching to DSC 13
*Feb 16 03:24:53.931:%DSC_REDUNDANCY-3-BICLINK:Failover:changing to active mode
*Feb 16 03:24:54.931:%DIAL13-3-MSG:
02:32:06:%DSC_REDUNDANCY-3-EVENT:Redundancy event:LINK_FAIL from other DSC
*Feb 16 03:24:55.491:%OIR-6-INSCARD:Card inserted in slot 12, interfaces administratively
shut down
*Feb 16 03:24:58.455:%DIAL13-3-MSG:
02:32:09:%DSC_REDUNDANCY-3-EVENT:Redundancy event:LINK_FAIL from other DSC
*Feb 16 03:25:04.939:%DIAL13-0-MSG:
RouterB# show redundancy
failover mode enabled, failover group = 32
Currently ACTIVE role.
No connection to slot 12
DSC in slot 13:
Hub is in 'active' state.
Clock is in 'backup' state.
RouterB# show redundancy history
DSC Redundancy Status Change History:
010216 03:09 Slot -1 DSC:Failover configured -> BACKUP role.
010216 03:24 Slot 13 DSC:Failover -> ACTIVE role.
010216 03:24 Slot 13 DSC:Hub, becoming active - D12 linkfail
010216 03:24 Slot 13 DSC:Hub, becoming active - D12 linkfail
*Feb 16 03:26:14.079:%DSIPPF-5-DS_HELLO:DSIP Hello from shelf 47 slot 1 Succeeded
*Feb 16 03:26:14.255:%DSIPPF-5-DS_HELLO:DSIP Hello from shelf 47 slot 3 Succeeded
*Feb 16 03:26:14.979:%DSIPPF-5-DS_HELLO:DSIP Hello from shelf 47 slot 10 Succeeded
```

Example: Privileged EXEC Mode

The following is sample output generated by this command in privileged EXEC mode on router platforms that support no keywords for the privileged EXEC mode form of the command:

```
RouterB# show redundancy
MWR1900 is the Active Router
Previous States with most recent at bottom
 INITL_INITL     Dec 31 19:00:00.000
 LISTN_INITL     Feb 28 19:00:15.568
```

```
LISTN_LISTN     Feb 28 19:00:15.568
SPEAK_LISTN     Feb 28 19:00:18.568
SPEAK_SPEAK     Feb 28 19:00:18.568
STDBY_SPEAK     Mar 19 08:54:26.191
ACTIV_SPEAK     Mar 19 08:54:26.191
ACTIV_STDBY     Mar 19 08:54:26.191
ACTIV_ACTIV     Mar 19 08:54:26.191
INITL_ACTIV     Mar 19 08:56:22.700
INITL_INITL     Mar 19 08:56:22.700
INITL_LISTN     Mar 19 08:56:28.544
LISTN_LISTN     Mar 19 08:56:28.652
LISTN_SPEAK     Mar 19 08:56:31.544
SPEAK_SPEAK     Mar 19 08:56:31.652
SPEAK_STDBY     Mar 19 08:56:34.544
SPEAK_ACTIV     Mar 19 08:56:34.544
STDBY_ACTIV     Mar 19 08:56:34.652
ACTIV_ACTIV     Mar 19 08:56:34.652
INITL_ACTIV     Mar 19 10:20:41.455
INITL_INITL     Mar 19 10:20:41.455
INITL_LISTN     Mar 19 10:20:49.243
LISTN_LISTN     Mar 19 10:20:49.299
LISTN_SPEAK     Mar 19 10:20:52.244
SPEAK_SPEAK     Mar 19 10:20:52.300
SPEAK_STDBY     Mar 19 10:20:55.244
STDBY_STDBY     Mar 19 10:20:55.300
ACTIV_STDBY     Mar 19 10:21:01.692
ACTIV_ACTIV     Mar 19 10:21:01.692
```

Related Commands

Command	Description
debug redundancy	Displays information used for troubleshooting dual (redundant) router shelves (Cisco AS5800) or RSCs (Cisco AS5850).
hw-module	Enables the router shelf to stop a DSC or to restart a stopped DSC.
mode	Sets the redundancy mode.
mode y-cable	Invokes y-cable mode.
redundancy	Enters redundancy configuration mode.
redundancy force-switchover	Forces a switchover from the active to the standby supervisor engine.
show chassis	Displays, for a router with two RSCs, information about the mode (handover-split or classic-split), RSC configuration, and slot ownership.
show standby	Displays the standby configuration.
standalone	Specifies whether the MWR 1941-DC router is used in a redundant or standalone configuration.
standby	Sets HSRP attributes.

show redundancy (HSA redundancy)

To display the current redundancy mode, use the **showredundancy**command in user EXEC or privileged EXEC mode.

show redundancy

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
11.2 GS	This command was introduced.
12.0(16)ST	This command was modified to display information about Route Processor Redundancy (RPR).
12.0(19)ST1	This command was modified to display information about RPR Plus (RPR+).
12.3(7)T	The command modifications to support RPR and RPR+ were integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

Use this command to display the redundancy mode of a Cisco 7500 series router. The default redundancy mode is High System Availability (HSA). Use the **redundancy**configuration command to enter redundancy configuration mode. Use the **moderpr**command in redundancy configuration mode to configure RPR as the high availability mode. HSA is the default high availability mode.

Examples

The following is sample output from the **showredundancy** command for a router with RPR configured:

```
Router# show redundancy
redundancy mode rpr
hw-module slot 2 image slot0:rsp-pv-mz
hw-module slot 3 image slot0:rsp-pv-mz
```

Related Commands

Command	Description
hw-module sec-cpu reset	Resets and reloads the standby RSP with the specified Cisco IOS image and executes the image.
hw-module slot image	Specifies a high availability Cisco IOS image to run on a standby RSP.
mode (HSA redundancy)	Configures the redundancy mode.
redundancy	Enters redundancy configuration mode.

show redundancy interchassis

To display information about interchassis redundancy group configuration, use the **show redundancy interchassis** command in privileged EXEC mode.

show redundancy interchassis *group-number*

Syntax Description

group-number	Interchassis redundancy group number.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS 15.2(1)S	This command was introduced.
Cisco IOS XE 3.11S	This command was integrated into Cisco IOS XE Release 3.11S.

The following is sample output from the **show redundancy interchassis** command when *group-number* is used to display information about an interchassis redundancy group:

```
Router# show redundancy interchassis 100

Redundancy Group 100 (0x64)
Applications connected: MR-APS with HSPW
Monitor mode: RW
member ip: 60.60.60.2 "R-222-2028", CONNECTED
Route-watch for 60.60.60.2 is UP
MR-APS with HSPW state: CONNECTED
backbone int GigabitEthernet0/4/0: UP (IP)
backbone int GigabitEthernet0/4/2: UP (IP)
ICRM fast-failure detection neighbor table
IP Address Status Type Next-hop IP Interface
========== ====== ==== =========== =========
60.60.60.2 UP RW
```

Related Commands

Command	Description
show hspw-aps-icrm	Displays information about HSPW.

show redundancy interlink

To display interlink utilization, use the **showredundancyinterlink**command in user EXEC or privileged EXEC mode.

show redundancy interlink [{**rx** | **tx** [{**pps** | **bps**}]}] [**histogram**]

Syntax Description

rx	(Optional) Receive interlink utilization histograms.
tx	(Optional) Transmit interlink utilization histograms.
pps	(Optional) Packets per second (pps) histograms.
bps	(Optional) Bytes per second (bps) histograms.
histogram	(Optional) Usage information.

Command Default

Interlink utilization information is not displayed.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco AS5850.
12.2(31)SB	This command was introduced on the Cisco 10000 series Internet routers. Support for the Cisco AS5850 is not included in this release.

Usage Guidelines

Use the **showredundancyinterlink** command to display the current or historical status on interlink utilization.

Examples

The following histogram displays receive BPS interlink information for the past minute, the past hour, and the past three days:

```
Router# show redundancy interlink rx bps histogram
      111111111111111111111111111111111111111111111111112222222222111
5000
4500
4000
3500
3000
2500
2000
1500
1000
  500
     0....5....1....1....2....2....3....3....4....4....5....5....
               0    5    0    5    0    5    0    5    0    5
                    Interlink Rx BPS (last 60 seconds)
                       # = Bits Per Second (x1000)
      211111211111212111112111111121111111111111111111111111111
5000
4500
```

```
4000
3500
3000
2500
2000
1500
1000
  500
     0....5....1....1....2....2....3....3....4....4....5....5....
               0    5    0    5    0    5    0    5    0    5
                    Interlink Rx BPS (last 60 minutes)
            * = maximum BPS (x1000)    # = average BPS (x1000)

111122222111111111211111111111111112112111111111111111211121111111111111
5000
4500
4000
3500
3000
2500
2000
1500
1000
  500

0....5....1....1....2....2....3....3....4....4....5....5....6....6....7.
               0    5    0    5    0    5    0    5    0    5    0
5    0
                    Interlink Rx BPS (last 72 hours)
            * = maximum BPS (x1000)    # = average BPS (x1000)
```

show rpc

To display remote procedure call (RPC) information, use the **showrpc** command in user EXEC or privileged EXEC mode.

show rpc {**applications** | **counters** | **status**}

Syntax Description

applications	Displays information about the RPC application.
counters	Displays the RPC counters.
status	Displays the RPC status.

Command Default

This command has no default settings.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to display RPC applications:

```
Router#
show rpc applications
  ID Dest Callback Application
   1 0011 <remote> rpc-master
   2 0011 <remote> cygnus-oir
   3 0021 60201708 rpc-slave-33
   4 0021 6022A514 idprom-MP
   5 0021 60204420 msfc-oir
   6 0011 <remote> Nipcon-SP
   7 0011 <remote> sw_vlan_sp
   8 0011 <remote> stp_switch_api
   9 0011 <remote> pagp_rpc
  10 0011 <remote> span_switch_rpc
  11 0011 <remote> pf_rp_rpc
  13 0011 <remote> mapping_sp
  14 0011 <remote> logger-sp
  17 0011 <remote> c6k_power_sp
  18 0011 <remote> c6k_sp_environmental
  19 0011 <remote> pagp_switch_rpc
  20 0011 <remote> pm-cp
  21 0021 602675B0 Nipcon-RP
  22 0021 602283B0 pm-mp
  23 0021 601F2538 sw_vlan_rp
  24 0021 601F77D0 span_switch_sp_rpc
  25 0021 601F7950 idbman_fec
  26 0021 601F7F30 logger-rp
  27 0021 601F80D8 pagp_switch_l3_split
```

```
  28 0021 601F81C0 pagp_switch_sp2mp
  29 0021 6026F190 c6k_rp_environmental
Router#
```

This example shows how to display information about the RPC counters:

```
Router#
show rpc counters
  ID Dest Rcv-req  Xmt-req  Q size   Application
   1 0011 0        26       0        rpc-master
   2 0011 0        6221     0        cygnus-oir
   4 0021 15       0        0        idprom-MP
   5 0021 6222     0        0        msfc-oir
   7 0011 0        2024     0        sw_vlan_sp
   8 0011 0        3        0        stp_switch_api
   9 0011 0        188      0        pagp_rpc
  11 0011 0        4        0        pf_rp_rpc
  13 0011 0        2        0        mapping_sp
  14 0011 0        3        0        logger-sp
  17 0011 0        2        0        c6k_power_sp
  18 0011 0        66       0        c6k_sp_environmental
  19 0011 0        109      0        pagp_switch_rpc
  20 0011 0        33       0        pm-cp
  22 0021 126      0        0        pm-mp
  23 0021 5        0        0        sw_vlan_rp
  24 0021 14       0        0        span_switch_sp_rpc
  25 0021 22       0        0        idbman_fec
  26 0021 8        0        0        logger-rp
  27 0021 3        0        0        pagp_switch_l3_split
  28 0021 3        0        0        pagp_switch_sp2mp
Router#
```

show running configuration | include mode

Use this command to configure hardware module of the chassis.

show running configuration | include mode

There are no keywords for this command.

Command Default

None

Command Modes

User EXEC Privileged EXEC

Examples

The following example shows how to configure configure 5G mode from 10G mode:

```
enable
configure terminal
platform hw-module configuration
hw-module slot / bay PID mode 5G_CEM
end
```

Related Commands

Command	Description
platform hw-module configuration	Configures the hardware module of the chassis
hw-module mode	Configures the IM from 10G to 5G mode.

show scp

To display Switch-Module Configuration Protocol (SCP) information, use the **show scp** in privileged EXEC mode on the Switch Processor.

show scp {**accounting** | **counters** | **linecards** [**details**] | **mcast** {**group** *group-id* | **inst**} | **process** *id* | **status**}

Syntax Description

accounting	Displays information about the SCP accounting.
counters	Displays information about the SCP counter.
linecards	Displays information about the Optical Services Module (OSM) wide area network (WAN) modules in the chassis.
details	(Optional) Displays detailed information about the OSM WAN module.
mcast	Displays information about the SCP multicast.
group *group-id*	(Optional) Displays information for a specific group and group ID; valid values are from 1 to 127.
inst	(Optional) Displays information for an instance.
process *id*	Displays all the processes that have registered an SAP with SCP.
status	Displays information about the local SCP server status.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC on the Switch Processor

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXE	The output of the **show scp process** command was changed to display all the processes that have registered an SAP with SCP on the Supervisor Engine 720 only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.0(1)S	The output of the **show scp status** command was changed to additionally display the Flow Control State (FC-State) and the Flow Control Count (FC-Count)

Examples

This example displays the SCP flow control status:

```
Router# show scp status
Rx 185,  Tx 181,  scp_my_addr 0x14
```

```
Id Sap   Channel name      current/peak/retry/dropped/totaltime(queue/process/ack) FC-state
  FC-count
-------------------------------------------------------------  --------- ---- -------
 0  18   SCP Unsolicited:18    801/    0/     0/      0/     0      0/   0/   0 off        0
 1  80   SCP Unsolicited:80      0/    0/     0/      0/     0      0/   0/   0 off        0
 2  23   SCP async: LCP#5        0/    0/     0/      0/     0      0/   0/   0 off        0
 3  0    SCP Unsolicited:0       0/    1/     0/      0/     5      0/   0/   0 off        0

------------------------------------------------------------------------------------------------------------------------
```

FC-state indicates the flow control state and FC-count indicates the number of times flow control has been turned on.

This example shows how to display all the processes that have registered an SAP with SCP:

```
Router# show module
Mod Ports Card Type                              Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
  1   48  48-port 10/100 mb RJ45                 WS-X6148-RJ-45     SAL091800RY
  2    0  2 port adapter Enhanced FlexWAN        WS-X6582-2PA       JAE0940MH7Z
  3    8  8 port 1000mb GBIC Enhanced QoS        WS-X6408A-GBIC     SAL09391KZH
  5    2  Supervisor Engine 720 (Active)         WS-SUP720-3BXL     SAL09337UE6
  6    2  Supervisor Engine 720 (Hot)            WS-SUP720-3BXL     SAL09148P59
Mod MAC addresses                       Hw    Fw           Sw           Status
--- ---------------------------------- ------ ------------ ------------ -------
  1  0013.c3f8.d2c4 to 0013.c3f8.d2f3   5.0   8.3(1)       8.6(0.366)TA Ok
  2  0015.2bc3.5b40 to 0015.2bc3.5b7f   2.1   12.2(nightly 12.2(nightly Ok
  3  0015.6324.ed48 to 0015.6324.ed4f   3.1   5.4(2)       8.6(0.366)TA Ok
  5  0014.a97d.b0ac to 0014.a97d.b0af   4.3   8.4(2)       12.2(nightly Ok
  6  0013.7f0d.0660 to 0013.7f0d.0663   4.3   8.4(2)       12.2(nightly Ok
Mod  Sub-Module                  Model              Serial       Hw     Status
---- --------------------------- ------------------ ----------- ------- -------
  5  Policy Feature Card 3       WS-F6K-PFC3BXL     SAL09337NVE  1.6    Ok
  5  MSFC3 Daughterboard         WS-SUP720          SAL09327AU6  2.3    Ok
  6  Policy Feature Card 3       WS-F6K-PFC3BXL     SAL1033Y0YK  1.8    Ok
  6  MSFC3 Daughterboard         WS-SUP720          SAL09158XB3  2.3    Ok
Mod  Online Diag Status
---- -------------------
  1  Pass
  2  Pass
  3  Pass
  5  Pass
  6  Pass
Router# attach 5
Trying Switch ...
Entering CONSOLE for Switch
Type "^C^C^C" to end this session
Switch-sp#
show scp process
Sap Pid Name
=== === ====
0 180 CWAN-RP SCP Input Process
18 42 itasca
20 3 Exec
21 3 Exec
22 180 CWAN-RP SCP Input Process
Total number of SAP registered = 5
Router#
```

show service-module serial through standby port

show service-module serial

To display the performance report for an integrated CSU/DSU, use the **showservice-moduleserial** command in privileged EXEC mode.

show service-module serial *number* [**performance-statistics** [*interval-range*]]

Syntax Description

number	Interface number 0 or 1.
performance-statistics	(Optional) Displays the CSU/DSU performance statistics for the past 24 hours. This keyword applies only to the fractional T1/T1 module.
interval-range	(Optional) Specifies the number of 15-minute intervals displayed. You can choose a range from 1 to 96, where each value represents the CSU/DSU activity performed in that 15-minute interval. For example, a range of 2-3 displays the performance statistics for the intervals two and three.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command applies to the 2- and 4-wire 56/64-kbps CSU/DSU module and FT1/T1 CSU/DSU module. The **performance-statistics** keyword applies only to the FT1/T1 CSU/DSU module.

Examples

The following sample output shows CSU/DSU performance statistics on a Cisco 2524 or Cisco 2525 router for intervals 30 to 32. Each interval is 15 minutes long. All the data is zero because no errors were discovered on the T1 line:

```
Router#
show service-module serial 1 performance-statistics 30-32
Total Data (last 58 15 minute intervals):
    0 Line Code Violations, 0 Path Code Violations
    0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
Data in current interval (131 seconds elapsed):
    0 Line Code Violations, 0 Path Code Violations
    0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
Data in Interval 30:
    0 Line Code Violations, 0 Path Code Violations
    0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
Data in Interval 31:
    0 Line Code Violations, 0 Path Code Violations
    0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
```

```
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
Data in Interval 32:
    0 Line Code Violations, 0 Path Code Violations
    0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
```

The following is sample output from the **showservice-moduleserial**command for a fractional T1 line:

```
Router1# show service-module serial 0
Module type is T1/fractional
    Hardware revision is B, Software revision is 1.1 ,
    Image checksum is 0x2160B7C, Protocol revision is 1.1
Receiver has AIS alarm,
Unit is currently in test mode:
    line loopback is in progress
Framing is ESF, Line Code is B8ZS, Current clock source is line,
Fraction has 24 timeslots (64 Kbits/sec each), Net bandwidth is 1536 Kbits/sec.
Last user loopback performed:
    remote loopback
    Failed to loopup remote
Last module self-test (done at startup): Passed
Last clearing of alarm counters 0:05:50
    loss of signal        :    1, last occurred 0:01:50
    loss of frame         :    0,
    AIS alarm             :    1, current duration 0:00:49
    Remote alarm          :    0,
    Module access errors  :    0,
Total Data (last 0 15 minute intervals):
Line Code Violations, 0 Path Code Violations
    0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
Data in current interval (351 seconds elapsed):
    1466 Line Code Violations, 0 Path Code Violations
    25 Slip Secs, 49 Fr Loss Secs, 40 Line Err Secs, 1 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 49 Unavail Secs
```

The following sample output from the **showservice-moduleserial**command displays the status of a switched 56-KB line:

```
Router1# show service-module serial 1
Module type is 4-wire Switched 56
    Hardware revision is B, Software revision is 1.00,
    Image checksum is 0x44453634, Protocol revision is 1.0
Connection state: active,
Receiver has loss of signal, loss of sealing current,
Unit is currently in test mode:
    line loopback is in progress
Current line rate is 56 Kbits/sec
Last user loopback performed:
    dte loopback
    duration 00:00:58
Last module self-test (done at startup): Passed
Last clearing of alarm counters 0:13:54
    oos/oof               :    3, last occurred 0:00:24
    loss of signal        :    3, current duration 0:00:24
    loss of sealing curren:    2, current duration 0:04:39
    loss of frame         :    0,
    rate adaption attempts:    0,
```

The following shows sample output from the **showservice-moduleserial**command issued on a Cisco 3640 modular access router:

```
Router# show service-module serial 0/1
Module type is 4-wire Switched 56
    Hardware revision is B, Software revision is 1.00,
    Image checksum is 0x42364436, Protocol revision is 1.0
Connection state: Idle
Receiver has no alarms.
CSU/DSU Alarm mask is 0
Current line rate is 56 Kbits/sec
Last module self-test (done at startup): Passed
Last clearing of alarm counters 4d02h
    oos/oof              :    0,
    loss of signal       :    0,
    loss of sealing curren:    0,
    loss of frame        :    0,
    rate adaptation attemp:    0,
```

The following shows sample output from the **showservice-moduleserial**command issued on a Cisco 1605 router:

```
Router# show service-module serial 0
Module type is 4-wire Switched 56
    Hardware revision is B, Software revision is 1.00,
    Image checksum is 0x42364436, Protocol revision is 1.0
Receiver has oos/oof, loss of signal,
CSU/DSU Alarm mask is 4
Current line rate is 56 Kbits/sec
Last module self-test (done at startup): Passed
Last clearing of alarm counters 1d02h
    oos/oof              :    1, current duration 1d02h
    loss of signal       :    1, current duration 1d02h
    loss of frame        :    0,
    rate adaptation attemp:    0,
```

The table below describes the fields displayed by the **showservice-moduleserial**command.

Table 265: show service-module serial Field Descriptions

Field	Description
Module type	CSU/DSU module installed in the router. The possible modules are T1/fractional, 2-wire switched 56-kbps, and 4-wire 56/64-kbps.

Field	Description		
Receiver has AIS alarm	Alarms detected by the FT1/T1 CSU/DSU module or 2- and 4-wire 56/64-kbps CSU/DSU modules. Possible T1 alarms are as follows: • Transmitter is sending remote alarm. • Transmitter is sending AIS. • Receiver has loss of signal. • Receiver has loss of frame. • Receiver has remote alarm. • Receiver has no alarms. Possible switched 56k alarms are as follows: • Receiver has loss of signal. • Receiver has loss of sealing current. • Receiver has loss of frame. • Receiver has rate adaptation attempts.	Unit is currently in test mode	Loopback tests are in progress.
		Framing	Indicates frame type used on the line. Can be extended super frame or super frame.
		Line Code	Indicated line-code type configured. Can be alternate mark inversion (AMI) or binary 8-zero substitution (B8ZS).
		Current clock source	Clock source configured on the line, which can be supplied by the service provider (line) or the integrated CSU/DSU module (internal).
		Fraction	Number of time slots defined for the FT1/T1 module, which can range from 1 to 24.
		Net bandwidth	Total bandwidth of the line (for example, 24 time slots multiplied by 64 kbps equals a bandwidth of 1536 kbps).
		Last user loopback performed	Type and outcome of the last performed loopback.
		Last module self-test (done at startup): Passed	Status of the last self-test performed on an integrated CSU/DSU module.
Last clearing of alarm counters	List of network alarms that were detected and cleared on the CSU/DSU module.		
Total Data Data in current interval	Shows the current accumulation period, which rolls into the 24-hour accumulation every 15 minutes. The oldest 15-minute period falls off the back of the 24-hour accumulation buffer.		

Field	Description
Line Code Violations	Indicates the occurrence of either a bipolar violation or excessive zeroes error event.
Path Code Violations	Indicates a frame synchronization bit error in the D4 and E1-no cyclic redundancy checksum (CRC) formats or a CRC error in the extended super frame (ESF) and E1-CRC formats.
Slip Secs	Indicates the replication or detection of the payload bits of a DS1 frame. A slip may be performed when there is a difference between the timing of a synchronous receiving terminal and the received signal.
Fr Loss Secs	Indicates the number of seconds an Out-of-Frame error is detected.
Line Err Secs	Line errored seconds is a second in which one or more line code violation errors are detected.
Errored Secs	In ESF and E1-CRC links, an errored second is a second in which one of the following is detected: one or more path code violations; one or more Out-of-Frame defects; one or more controlled slip events; a detected AIS defect. For D4 and E1-no-CRC links, the presence of bipolar violation also triggers an errored second.
Bursty Err Secs	Second with fewer than 320 and more than 1 path coding violation errors. No severely errored frame defects or incoming AIS defects are detected. Controlled slips are not included in this parameter.
Severely Err Secs	For ESF signals, a second with one of the following errors: 320 or more path code violation errors; one or more Out-of-Frame defects; a detected AIS defect. For D4 signals, a count of 1-second intervals with framing errors, or an Out-of-Frame defect, or 1544 line code violations.
Unavail Secs	Total time the line was out of service.

Related Commands

Command	Description
clear service-module serial	Resets an integrated CSU/DSU.

show sip-disk

To display file information on the internal storage disk of the SPA interface processor (SIP), use the **showsip-disk** command in privileged EXEC configuration mode.

show sip *slot-disk0* [{**all** | **chips** | **filesys**}]

Syntax Description

slot	Chassis slot number. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding “Identifying Slots and Subslots for SIPs and SPAs” topic in the platform-specific SPA software configuration guide.
all	(Optional) Displays all information on the Flash Disk.
chips	(Optional) Displays information for files on the Flash Disk. This is the default.
filesys	(Optional) Displays file system parameters for the Flash Disk.

Command Default

If no optional keyword is specified, information for files on the Flash Disk is the default display (same as using the **chips** keyword).

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	Thiscommand was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example shows information about eight files stored internally on the SIP located in slot 5 of the router:

```
Router# show sip5-disk0
-#- --length-- -----date/time------ path
 number of file 8
 inode path is 1 idprom-oc12-atm-superspa
 fullpath is disk0:/idprom-oc12-atm-superspa
1         1152 Jun 09 2004 13:03:38 idprom-oc12-atm-superspa
 inode path is 2 idprom-4oc3-atm-superspa
 fullpath is disk0:/idprom-4oc3-atm-superspa
2         1152 Jun 09 2004 05:51:34 idprom-4oc3-atm-superspa
 inode path is 3 bonham_brd_rev2_rev19.hex
 fullpath is disk0:/bonham_brd_rev2_rev19.hex
3      2626407 Aug 24 2004 11:04:42 bonham_brd_rev2_rev19.hex
 inode path is 4 sip2-dw-mz.b2-testt
 fullpath is disk0:/sip2-dw-mz.b2-testt
4      5895640 Aug 26 2004 05:09:08 sip2-dw-mz.b2-testt
 inode path is 5 sip2-dw-mz.hp-depth
 fullpath is disk0:/sip2-dw-mz.hp-depth
5      5897476 Aug 12 2004 04:40:38 sip2-dw-mz.hp-depth
 inode path is 6 viking1.jbc
 fullpath is disk0:/viking1.jbc
```

```
6      2678150 Jun 09 2004 12:48:32 viking1.jbc
 inode path is 7 sip2-dw-mz.hpd
 fullpath is disk0:/sip2-dw-mz.hpd
7      5916716 Aug 25 2004 10:25:14 sip2-dw-mz.hpd
 inode path is 8 sip2iofpga_promlatest_rev78.hex
 fullpath is disk0:/sip2iofpga_promlatest_rev78.hex
8       468975 Aug 24 2004 10:56:54 sip2iofpga_promlatest_rev78.hex
40606720 bytes available (23490560 bytes used)
```

The following example shows information about the SIP flash file system for the SIP located in slot 5 of the router:

```
Router# show sip3-disk0 filesys
******** ATA Flash Card Geometry/Format Info ********
ATA CARD GEOMETRY
   Number of Heads:       4
   Number of Cylinders    978
   Sectors per Cylinder   32
   Sector Size            512
   Total Sectors          125184
ATA CARD FORMAT
   Number of FAT Sectors  62
   Sectors Per Cluster    8
   Number of Clusters     15598
   Number of Data Sectors 125049
   Base Root Sector       227
   Base FAT Sector        103
   Base Data Sector       259
ATA MONLIB INFO
   Image Monlib size = 52216
   Disk monlib size = 52736
   Name = NA
   Monlib end sector = NA
   Monlib Start sector = NA
   Monlib updated by = NA
   Monlib version = NA
RFS VERSION :
Negotiated Version                  : 0
Highest version supported in Server : 0
Highest version supported in Client : 0
```

show slot0:

To display information about the PCMCIA flash memory card's file system located in slot 0, use the **show slot0:**command in user EXEC or privileged EXEC mode.

show slot0:[{**all** | **chips** | **detailed** | **err** | **summary**}]

Syntax Description

all	(Optional) Displays all possible flash system information for all PCMCIA flash cards in the system.
chips	(Optional) Displays flash chip information.
detailed	(Optional) Displays the flash detailed directory.
err	(Optional) Displays the flash chip erase and write retries.
summary	(Optional) Displays the flash partition summary.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **show slot0:** command to display details about the files in a particular linear PCMCIA flash memory card of less than 20 MB and some 32 MB linear PCMCIA cards.

Note Use the **show disk** command for ATA PCMCIA cards. Other forms of this commands are **show disk0:** and **show disk1:**.

For more information regarding file systems and flash cards, access the *PCMCIA Filesystem Compatibility Matrix and Filesystem Information* document at the following URL:

http://www.cisco.com/en/US/partner/products/hw/routers/ps341/products_tech_note09186a00800a7515.shtml

To see which flash cards are used in your router, use the **show version** command and look at the bottom portion of the output.

The following display indicates an ATA PCMCIA flash disk.

```
Router# show version
.
.
46976K bytes of ATA PCMCIA card at slot 0 (Sector size 512 bytes).
```

The following display indicates a linear PCMCIA flash card with 20480K bytes of flash memory in card at slot 1 with a sector size of 128K.

```
Router# show version
.
.
20480K bytes of Flash PCMCIA card at slot 1 (Sector size 128K).
```

Note In some cases the **show slot** command will not display the file systems, use **show slot0:** or **show slot1:**.

Examples

The following example displays information about slot 0. The output is self-explanatory.

```
Router# show slot0:
PCMCIA Slot0 flash directory:
File  Length   Name/status
  1   11081464  c3660-bin-mz.123-9.3.PI5b
[11081528 bytes used, 9627844 available, 20709372 total]
20480K bytes of processor board PCMCIA Slot0 flash (Read/Write)
Router# show slot0: all
Partition   Size    Used      Free      Bank-Size  State          Copy Mode
  1        20223K  10821K     9402K     4096K      Read/Write     Direct
PCMCIA Slot0 flash directory:
File  Length   Name/status
        addr      fcksum  ccksum
  1   11081464  c3660-bin-mz.123-9.3.PI5b
        0x40      0x5EA3  0x5EA3
[11081528 bytes used, 9627844 available, 20709372 total]
20480K bytes of processor board PCMCIA Slot0 flash (Read/Write)
   Chip    Bank    Code      Size      Name
    1      1       89A0      2048KB    INTEL 28F016SA
    2      1       89A0      2048KB    INTEL 28F016SA
    1      2       89A0      2048KB    INTEL 28F016SA
    2      2       89A0      2048KB    INTEL 28F016SA
    1      3       89A0      2048KB    INTEL 28F016SA
    2      3       89A0      2048KB    INTEL 28F016SA
    1      4       89A0      2048KB    INTEL 28F016SA
    2      4       89A0      2048KB    INTEL 28F016SA
    1      5       89A0      2048KB    INTEL 28F016SA
    2      5       89A0      2048KB    INTEL 28F016SA
The following example shows flash chip information.
Router# show slot0: chips

20480K bytes of processor board PCMCIA Slot0 flash (Read/Write)
   Chip    Bank    Code      Size      Name
    1      1       89A0      2048KB    INTEL 28F016SA
    2      1       89A0      2048KB    INTEL 28F016SA
    1      2       89A0      2048KB    INTEL 28F016SA
    2      2       89A0      2048KB    INTEL 28F016SA
    1      3       89A0      2048KB    INTEL 28F016SA
    2      3       89A0      2048KB    INTEL 28F016SA
    1      4       89A0      2048KB    INTEL 28F016SA
    2      4       89A0      2048KB    INTEL 28F016SA
    1      5       89A0      2048KB    INTEL 28F016SA
    2      5       89A0      2048KB    INTEL 28F016SA
```

The following example show the flash detailed directory.

```
Router# show slot0: detailed
PCMCIA Slot0 flash directory:
File  Length   Name/status
```

```
        addr      fcksum  ccksum
  1   11081464  c3660-bin-mz.123-9.3.PI5b
        0x40      0x5EA3  0x5EA3
[11081528 bytes used, 9627844 available, 20709372 total]
20480K bytes of processor board PCMCIA Slot0 flash (Read/Write)
```

The following example shows the flash chip erase and write retries.

```
Router# show slot0: err

PCMCIA Slot0 flash directory:
File  Length   Name/status
  1   11081464  c3660-bin-mz.123-9.3.PI5b
[11081528 bytes used, 9627844 available, 20709372 total]
20480K bytes of processor board PCMCIA Slot0 flash (Read/Write)
   Chip    Bank    Code      Size      Name               erase  write
     1      1       89A0      2048KB    INTEL 28F016SA      0      0
     2      1       89A0      2048KB    INTEL 28F016SA      0      0
     1      2       89A0      2048KB    INTEL 28F016SA      0      0
     2      2       89A0      2048KB    INTEL 28F016SA      0      0
     1      3       89A0      2048KB    INTEL 28F016SA      0      0
     2      3       89A0      2048KB    INTEL 28F016SA      0      0
     1      4       89A0      2048KB    INTEL 28F016SA      0      0
     2      4       89A0      2048KB    INTEL 28F016SA      0      0
     1      5       89A0      2048KB    INTEL 28F016SA      0      0
     2      5       89A0      2048KB    INTEL 28F016SA      0      0
```

The following example shows the flash partition summary.

```
Router# show
 slot0: summary

Partition   Size    Used      Free      Bank-Size  State          Copy Mode
  1        20223K  10821K     9402K     4096K      Read/Write     Direct
20480K bytes of processor board PCMCIA Slot0 flash (Read/Write)
```

Related Commands

Command	Description
dir slot0:	Directory listing of files on a PCMCIA Flash card located in slot0.
dir slot1:	Directory listing of files on a PCMCIA Flash card located in slot1.
show slot1:	Displays information about the PCMCIA flash memory card's file system located in slot 1.
show slot	Displays information about the PCMCIA flash memory cards.

show smf

To display the configured software MAC address filter (SMF) on various interfaces of a router, use the **showsmf**command in user EXEC or privileged EXEC mode.

show **smf** [*interface-name*]

Syntax Description

interface-name	(Optional) Displays information about the specified interface. Choices can include **atm**, **ethernet**, **fastethernet**, **null**, **serial**, **tokenring**, and **async**.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced in a release prior to 10.0.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The SMF is active whenever the router is doing bridging or Integrated Routing and Bridging (IRB). MAC address filtering can be used as a security feature in bridging or switching environments.

Examples

The following is sample output from the **showsmf** command:

```
Router# show smf fastethernet
 Software MAC address filter on FastEthernet0/0.2
  Hash Len    Address      Matches  Act      Type
  0x00:  0 ffff.ffff.ffff         0 RCV Physical broadcast
  0x0C:  0 0100.0c00.0000         0 RCV ISL vLAN Multicast
  0x2A:  0 0900.2b01.0001         0 RCV DEC spanning tree
  0xA6:  0 0010.a6ae.6000         0 RCV Interface MAC address
  0xC1:  0 0100.0ccc.cccd         0 RCV SSTP MAC address
  0xC2:  0 0180.c200.0000         0 RCV IEEE spanning tree
  0xC2:  1 0180.c200.0000         0 RCV IBM spanning tree
  0xC2:  2 0100.0ccd.cdce         0 RCV VLAN Bridge STP
```

The table below describes the fields shown in the display.

Table 266: show smf Field Descriptions

Field	Description
Hash	Position in the hash table for this entry.
Len	Length of the entry.
Address	MAC address for the interface.
Matches	Number of hits for the address.

Field	Description
Act	Action taken. Values can be receive (RCV), forward (FWD), or discard (DIS).
Type	Type of MAC address.

show srp

To display Spatial Reuse Protocol (SRP) information, use the **showsrp** command in user EXEC or privileged EXEC mode.

Cisco IOS SR, SX, and XE Trains
show srp [{**counters** | **failures** | **ips** | **source-counters** | **srr** | **topology** | **transit**}]

Cisco IOS T Train
show srp [{**counters** | **ips** | **source-counters** | **topology**}]

Syntax Description

counters	(Optional) Displays counters for the packets received and transmitted on both sides of an SRP node.
ips	(Optional) Displays Intrusion Prevention System (IPS) information.
source-counters	(Optional) Displays source counter information.
topology	(Optional) Displays topology map information.
failures	(Optional) Displays self-detected failures.
srr	(Optional) Displays Simple RSS Reader (SRR) information.
transit	(Optional) Displays information about traffic buffer delays.

Command Default

If no keyword is specified, generic information about SRP is displayed.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.4(24)T	This command was introduced in a release earlier than Cisco IOS Release 12.4(24)T.
12.2(33)SRC	This command was modified and integrated into a release earlier than Cisco IOS Release 12.2(33)SRC. The **failures**, **srr**, and **transit** keywords were added.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples

The following is sample output from the **showsrptopology**command:

```
Router# show srp topology
 Topology Map for Interface: SRP2_3
  Topology pkt. sent every 60 sec.  (next pkt. after 13 sec.)
  Last received topology pkt. 00:03:45
  Last topology change was 01:20:21 ago
```

```
  Hops (outer ring)      MAC       IP Address   Wrapped SRR   Name
        0       0005.dd9b.0d05        0.0.0.0   No    found SRP4
        1       0005.dd9b.0105        0.0.0.0   No    found SRP5
RP/0/1/0:SRP4#   0005.dd9b.2505        0.0.0.0   No    found SRP1
```

The table below describes the significant fields shown in the display.

Table 267: show srp topology Field Descriptions

Field	Description
Hops (outer ring)	Total number of hops.
MAC	Displays the MAC address.
IP Address	Displays the IP address.
Wrapped	Indicates if the SRP ring is wrapped at a node or not: Yes or No. If yes, the packet is sent in the reverse direction.
SRR	Status of the SRR, found or not found.
Name	Displays the hostname of the router for the node.

The following is sample output from the **showsrpips**command:

```
Router# show srp ips
 IPS Information for Interface SRP2_3
 MAC Addresses
   Side A (Outer ring RX) neighbor 0005.dd9b.2505
   Side B (Inner ring RX) neighbor 0005.dd9b.0105
   Node MAC address 0005.dd9b.0d05
 IPS State
   Side A not wrapped
   Side B not wrapped
   Side A (Inner ring TX) IPS pkt. sent every 1 sec. (next pkt. after 1 sec.)
   Side B (Outer ring TX) IPS pkt. sent every 1 sec. (next pkt. after 1 sec.)
   IPS WTR period is 60 sec. (timer is inactive)
   Node IPS State: idle
 IPS Self Detected Requests           IPS Remote Requests
   Side A            IDLE               Side A IDLE
   Side B            IDLE               Side B IDLE
 IPS messages received
   Side A (Outer ring RX) { 0005.dd9b.2505,IDLE,SHORT}, TTL 255
   Side B (Inner ring RX) { 0005.dd9b.0105,IDLE,SHORT}, TTL 255
 IPS messages transmitted
   Side A (Inner ring TX) { 0005.dd9b.0d05,IDLE,SHORT}, TTL 255
   Side B (Outer ring TX) { 0005.dd9b.0d05,IDLE,SHORT}, TTL 255
```

The table below describes the significant fields shown in the display.

Table 268: show srp ips Field Descriptions

Field	Description
MAC Addresses	MAC address of the IPS interface.
IPS State	Information about the current IPS states.

Field	Description
IPS Self Detected Requests	Details about the IPS self-detected requests.
IPS Remote Requests	Details about the IPS remote requests.
IPS messages received	Details about the IPS messages received.
IPS messages transmitted	Details about the transmitted IPS messages.

Related Commands

Command	Description
clear counters srp	Clears SRP counters.
show interfaces srp	Displays the configuration on an SRP interface.
show srp counters	Displays counters for the packets received, transmitted, and transited on both sides of an SRP node.
show srp failures	Displays the IPS status.
show srp source-counters	Displays the total number of packets received by a node identified by its unique MAC address.
srp topology-timer	Specifies the frequency of the topology timer.

show storm-control

To display switchport characteristics, including storm-control levels set on the interface, use the **showstorm-control**command in user EXEC or privileged EXEC mode.

show storm-control [*interface-type interface-number*] [{**broadcast** | **multicast** | **unicast** | **history**}]

Syntax Description

interface-type interface-number	(Optional) Port for which information is to be displayed.
broadcast	(Optional) Displays broadcast storm information. This is the default.
multicast	(Optional) Displays multicast storm information.
unicast	(Optional) Displays unicast storm information.
history	(Optional) Displays storm history on a per-port basis.

Command Default

If the *interface-type* and *interface-number*values are omitted, the **showstorm-control** command displays storm-control settings for all ports on the switch.

You can display broadcast, multicast, or unicast packet-storm information by using the corresponding keyword. When no keyword option is specified, the default is to display broadcast storm-control information.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(2)XT	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T to support switchport creation on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(15)ZJ	This command was modified. The *interface-type* and *interface-number* arguments and the **broadcast**, **multicast**, **unicast**, and **history** keywords were added to support the Ethernet switch network module on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Examples

The following is partial sample output from the **showstorm-controlbroadcast**command:

```
Router# show storm-control broadcast
Interface  Filter State   Upper    Lower    Current
---------  -------------  -------  -------  -------
Fa0/1      <inactive>     100.00%  100.00%    0.00%
Fa0/2      <inactive>     100.00%  100.00%    0.00%
Fa0/3      <inactive>     100.00%  100.00%    0.00%
Fa0/4      Forwarding      30.00%   20.00%   20.32%
.
.
.
```

The table below describes the fields shown in the display.

Table 269: show storm-control broadcast Field Descriptions

Field	Description
Interface	Displays the ID of the interface.
Filter State	Displays the status of the filter: • Blocking--Storm control is enabled, a storm has occurred, and the action is filter. • Forwarding--Storm control is enabled, and a storm has not occurred. • Inactive--Storm control is disabled. • Shutdown--Storm control is enabled, a storm has occurred, and the action is to shut down. **Note** If an interface is disabled by a broadcast, multicast, or unicast storm, the filter state for all traffic types is *shutdown* .
Upper	Displays the rising suppression level as a percentage of total available bandwidth.
Lower	Displays the falling suppression level as a percentage of total available bandwidth.
Current	Displays the bandwidth utilization of a specific traffic type as a percentage of total available bandwidth. This field is valid only when storm control is enabled.

The following is sample output from the **showstorm-controlfastethernet0/4history** command, which displays the ten most recent storm events for an interface:

```
Router# show storm-control fastethernet 0/4 history
 Interface Fa0/4 Storm Event History
 Event Type          Event Start Time  Duration (seconds)
 ------------------  ----------------  ------------------
 Unicast             04:58:18          206
 Broadcast           05:01:54          n/a
 Multicast           05:01:54          n/a
 Unicast             05:01:54          108
 Broadcast           05:05:00          n/a
 Multicast           05:05:00          n/a
 Unicast             05:06:00          n/a
 Broadcast           05:09:39          n/a
 Multicast           05:09:39          n/a
 Broadcast           05:11:32          172
```

The table below describes the fields shown in the display.

Table 270: show storm-control history Field Descriptions

Field	Description
Interface	Displays the ID of the interface.

Field	Description
Event Type	Displays the type of storm event. The event type is one of the following: • Broadcast • Multicast • Unicast
Event Start Time	Time when the event started, in hours, minutes, seconds.
Duration (seconds)	Duration time of the event, in seconds. **Note** The duration field could be *n/a* when a storm is still present or when a new storm of a different type occurs before the current storm ends.

Related Commands

Command	Description
show interface counters	Displays the count of discarded packets.
storm control	Enables broadcast, multicast, or unicast storm control on a port.

show sup-bootflash

To display information about the sup-bootflash file system, use the **show sup-bootflash** command in privileged EXEC mode.

show **sup-bootflash** [{**all** | **chips** | **filesys**}]

Syntax Description

all	(Optional) Displays all possible Flash information.
chips	(Optional) Displays information about the Flash chip.
filesys	(Optional) Displays information about the file system.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.217d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to display a summary of bootflash information:

```
Router#
show sup-bootflash
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
1   .. image    EBC8FC4D  A7487C    6 10700796 Nov 19 1999 07:07:37 halley
2   .. unknown  C7EB077D  EE2620   25  4644130 Nov 19 1999 07:50:44 cat6000-sup_
5-3-3-CSX.bin
645600 bytes available (15345184 bytes used)
Router#
```

This example shows how to display all bootflash information:

```
Router#
show sup-bootflash all
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
1   .. image    EBC8FC4D  A7487C    6 10700796 Nov 19 1999 07:07:37 halley
2   .. unknown  C7EB077D  EE2620   25  4644130 Nov 19 1999 07:50:44 cat6000-sup_
5-3-3-CSX.bin
645600 bytes available (15345184 bytes used)
-------- F I L E   S Y S T E M   S T A T U S --------
  Device Number = 2
DEVICE INFO BLOCK: bootflash
  Magic Number          = 6887635   File System Vers = 10000    (1.0)
  Length                = 1000000   Sector Size      = 40000
  Programming Algorithm = 19        Erased State     = FFFFFFFF
  File System Offset    = 40000     Length = F40000
  MONLIB Offset         = 100       Length = F568
```

```
  Bad Sector Map Offset = 3FFF8     Length = 8
  Squeeze Log Offset    = F80000    Length = 40000
  Squeeze Buffer Offset = FC0000    Length = 40000
  Num Spare Sectors     = 0
    Spares:
STATUS INFO:
  Writable
  NO File Open for Write
  Complete Stats
  No Unrecovered Errors
  No Squeeze in progress
USAGE INFO:
  Bytes Used     = EA2620  Bytes Available = 9D9E0
  Bad Sectors    = 0       Spared Sectors  = 0
  OK Files       = 2       Bytes = EA2520
  Deleted Files  = 0       Bytes = 0
  Files w/Errors = 0       Bytes = 0
******** Intel SCS Status/Register Dump ********
COMMON MEMORY REGISTERS: Bank 0
  Intelligent ID Code  : 890089
  Compatible Status Reg: 800080
DEVICE TYPE:
  Layout                 : Paired x16 Mode
  Write Queue Size       : 64
  Queued Erase Supported : No
Router#
```

This example shows how to display information about the Flash chip:

```
Router# show sup-bootflash chips
******** Intel SCS Status/Register Dump ********
COMMON MEMORY REGISTERS: Bank 0
  Intelligent ID Code  : 890089
  Compatible Status Reg: 800080
DEVICE TYPE:
  Layout                 : Paired x16 Mode
  Write Queue Size       : 64
  Queued Erase Supported : No
Router#
```

This example shows how to display information about the file system:

```
Router# show sup-bootflash filesys
-------- F I L E   S Y S T E M   S T A T U S --------
  Device Number = 2
DEVICE INFO BLOCK: bootflash
  Magic Number          = 6887635   File System Vers = 10000    (1.0)
  Length                = 1000000   Sector Size      = 40000
  Programming Algorithm = 19        Erased State     = FFFFFFFF
  File System Offset    = 40000     Length = F40000
  MONLIB Offset         = 100       Length = F568
  Bad Sector Map Offset = 3FFF8     Length = 8
  Squeeze Log Offset    = F80000    Length = 40000
  Squeeze Buffer Offset = FC0000    Length = 40000
  Num Spare Sectors     = 0
    Spares:
STATUS INFO:
  Writable
  NO File Open for Write
  Complete Stats
  No Unrecovered Errors
  No Squeeze in progress
USAGE INFO:
```

```
  Bytes Used     = EA2620  Bytes Available = 9D9E0
  Bad Sectors    = 0       Spared Sectors  = 0
  OK Files       = 2       Bytes = EA2520
  Deleted Files  = 0       Bytes = 0
  Files w/Errors = 0       Bytes = 0
Router#
```

show syscon sdp

To display information about the Shelf Discovery Protocol (SDP), use the **showsysconsdp**command in privileged EXEC or user EXEC mode.

show syscon sdp

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC User EXEC

Command History

Release	Modification
11.3AA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the**showsysconsdp** command:

```
Router# show syscon sdp
Current time 10:46:32 PST Jan 28 1998, system controller 172.23.66.100
Last hello packet received at 10:45:38 PST Jan 28 1998
11773 Total SDP packets
    0 packets with bad MD5 hash
    5884 Hello packets received
    5889 Hello packets sent
    0 Command packets received
    0 Command packets sent
```

The table below describes the fields shown in the sample display.

Table 271: show syscon sdp Field Descriptions

Field	Description
Current time	Current time and date.
system controller	IP address of the system controller.
Last hello packet received	Time and date when the last hello packet from the system controller was received by the shelf.
Total SDP packets	Total number of SDP packets sent or received by the shelf.
packets with bad MD5 hash	Number of packets with a bad MD5 hash.
Hello packets received	Number of hello packets received by the shelf from the system controller.
Hello packets sent	Number of hello packets sent from the shelf to the system controller.

Field	Description
Command packets received	Number of packets containing commands received by the shelf.
Command packets sent	Number of commands sent by the shelf.

Related Commands

Command	Description
syscon address	Specifies the system controller for a managed shelf.
syscon source-interface	Specifies the interface to use for the source address in SDP packets.

show system jumbomtu

To display the g lobal maximum transmission unit (MTU) setting, use the **show system jumbomtu** command in privileged EXEC mode.

show system jumbomtu

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to display the global MTU setting:

```
Router# show system jumbomtu
Global Ethernet MTU is 1550 bytes.
Router#
```

Related Commands

Command	Description
system jumbomtu	Sets the maximum size of the Layer 2 and Layer 3 packets.

show tcam counts

To display the Ternary Content Addressable Memory (TCAM) statistics, use the **showtcamcounts** command in privileged EXEC mode.

show tcam counts [**detail**] [{**arp** | **ip** | **ipv6** | **mpls** | **other**}] [**module** *number*]

Syntax Description

detail	Displays detailed TCAM statistics.
arp	Displays TCAM statistics for ARP traffic.
ip	Displays TCAM statistics for IP traffic
ipv6	Displays TCAM statistics for IPv6 traffic
mpls	Displays TCAM statistics for MPLS traffic
other	Displays TCAM statistics for other traffic
module *number*	(Optional) Specifies the module number; see the "Usage Guidelines" section for valid values.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **module***number* keyword and argument designate the module and port number. Valid values for *number* depend on the chassis and module that are used. For example, if you have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 2 to 13 and valid values for the port number are from 1 to 48.

The display includes information about the per-bank TCAM utilization for the ACL/QoS TCAM for Cisco 7600 series routers that are configured with a Supervisor Engine 720 only.

Examples

This example shows how to display the TCAM statistics:

```
Router# show tcam counts
              Used        Free        Percent Used       Reserved
              ----        ----        ------------       --------
 Labels:         8         504             1
ACL_TCAM
--------
  Masks:         6        4090             0                    0
```

```
Entries:     37      32731           0                     0
QOS_TCAM
--------
  Masks:      3       4093           0                     0
Entries:     20      32748           0                     0
    LOU:      0        128           0
  ANDOR:      0         16           0
  ORAND:      0         16           0
    ADJ:      1       2047           0
Router#
```

The table below describes the fields that are shown in the example.

Table 272: show tcam counts Command Output Fields

Field	Description
Labels Used	Number of labels that are used (maximum of 512).
Labels Free	Number of free labels remaining.
Labels Percent Used	Percentage of labels that are used.
Masks Used	Number of masks that are used (maximum of 4096).
Masks Free	Number of free labels remaining.
Masks Percent Used	Percentage of masks that are used.
Entries Used	Number of labels that are used (maximum of 32767).
Entries Free	Number of free labels that are remaining.
Entries Percent Used	Percentage of entries that are used.

Related Commands

Command	Description
show tcam interfaces	Displays information about the interface-based Ternary Content Addressable Memory (TCAM).

show tcam interface

To display information about the interface-based Ternary Content Addressable Memory (TCAM), use the **showtcaminterface** command in privileged EXEC mode.

show tcam interface {*interface interface-number* | **null** *interface-number* | **vlan** *vlan-id* {**acl** {**in** | **out**} | **qos** {**type1** | **type2**} *type* [{**detail** | **module** *number*}]}}

Syntax Description

interface	(Optional) Interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **pos**, **atm**, and **ge-wan**.
interface-number	(Optional) Module and port number; see the "Usage Guidelines" section for valid values.
null *interface-number*	(Optional) Specifies the null interface; the valid value is **0**.
vlan *vlan-id*	(Optional) Specifies the VLAN; see the "Usage Guidelines" section for valid values.
acl in	(Optional) Displays the ACL-based incoming packets.
acl out	(Optional) Displays the ACL-based outgoing packets.
qos type1	(Optional) Displays the QoS-based Type 1 packets.
qos type2	(Optional) Displays the QoS-based Type 2 packets.
type	Specifies the protocol type to display; valid values are **arp**, **ipv4**, **ipv6**, **mpls**, and **other**.
detail	(Optional) Displays detailed information.
module *number*	(Optional) Specifies the module number.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX	This command was changed to support the **ipv6** keyword.
12.2(17b)SXA	This command was changed as follows: • Support for the **detail** keyword was added to display detailed information. • The output (without the **detail** keyword) was changed to include the match count for supervisor engines and DFCs that support ACL counters.

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **pos**, **atm**, and **ge-wan**keywords are supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2 only.

Use the clear mls acl counters command to clear the TCAM ACL match counters.

The match counts display is supported in PFC3BXL or PFC3B mode only.

Examples

This example shows how to display interface-based TCAM information:

```
Router# show tcam interface
 vlan 7 acl in ip
deny ip any any
permit ip 10.20.0.0 0.0.255.255 10.22.0.0 0.0.255.255
redirect ip 10.21.0.0 0.0.255.255 10.23.0.0 0.0.255.255
permit tcp 10.24.0.0 0.0.255.255 10.30.0.0 0.0.255.255
Fragments (1 match)
permit tcp 10.25.0.0 0.0.255.255 10.31.0.0 0.0.255.255
fragments
permit tcp 10.25.0.0 0.0.255.255 range 30000 30020 10.31.0.0
0.0.255.255 range 10000 10010 (102 matches)
permit tcp 10.24.0.0 0.0.255.255 eq 9000 10.30.0.0 0.0.255.255
eq telnet
deny ip any any
deny ip any any
Router#
```

This example shows how to display detailed TCAM information:

```
Router# show tcam interface
 fa5/2 acl in ip detail
--------------------------------------------------------------------------------
-----------------------------------
DPort - Destination Port   SPort - Source Port        TCP-F - U -URG
 Pro   - Protocol
I     - Inverted LOU       TOS   - TOS Value                - A -ACK
 rtr   - Router
MRFM  - M -MPLS Packet     TN    - T -Tcp Control           - P -PSH
 COD   - C -Bank Care Flag
      - R -Recirc. Flag          - N -Non-cachable          - R -RST
       - I -OrdIndep. Flag
      - F -Fragment Flag   CAP   - Capture Flag             - S -SYN
       - D -Dynamic Flag
      - M -More Fragments  F-P   - FlowMask-Prior.          - F -FIN
 T     - V(Value)/M(Mask)/R(Result)
X     - XTAG               (*)   - Bank Priority
--------------------------------------------------------------------------------
-----------------------------------
Interface: 1018   label: 1   lookup_type: 0
protocol: IP   packet-type: 0
+-+-----+---------------+---------------+---------------+---------------+-------
+---+----+-+---+--+---+---+
|T|Index|  Dest Ip Addr | Source Ip Addr|     DPort     |     SPort     | TCP-F
```

```
|Pro|MRFM|X|TOS|TN|COD|F-P|
+-+-----+---------------+---------------+---------------+--------------+-------
+---+----+-+---+--+---+---+
 V 18396         0.0.0.0         0.0.0.0       P=0             P=0        ------
   0 ---- 0   0 -- --- 0-0
 M 18404         0.0.0.0         0.0.0.0         0               0
   0 ---- 0   0
 R rslt: L3_DENY_RESULT                rtr_rslt: L3_DENY_RESULT
 V 36828         0.0.0.0         0.0.0.0       P=0             P=0        ------
   0 ---- 0   0 -- --- 0-0
 M 36836         0.0.0.0         0.0.0.0         0               0
   0 ---- 0   0
 R rslt: L3_DENY_RESULT (*)            rtr_rslt: L3_DENY_RESULT (*)
Router#
```

Related Commands

Command	Description
clear mls acl counters	Clears the MLS ACL counters.
show tcam counts	Displays the Ternary Content Addressable Memory (TCAM) statistics.

show tcam-mgr subslot

To display ternary content addressable memory (TCAM) manager information for a SPA, use the **showtcam-mgrsubslot**command in privileged EXEC configuration mode.

show tcam-mgr subslot *slot/subslot* **inst-info**
show tcam-mgr subslot *slot/subslot* **region** *region-number* [{**config** | **statistics**}]
show tcam-mgr subslot *slot/subslot* {**rx-dest-mac** | **rx-vlan**} {**alloc-mbus** [**summary**] | **table**}
show tcam-mgr subslot *slot/subslot* **statistics**

Syntax Description

slot	Chassis slot number. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding “Identifying Slots and Subslots for SIPs and SPAs” topic in the platform-specific SPA software configuration guide.
/ *subslot*	Secondary slot number on a SIP where a SPA is installed. Refer to the platform-specific SPA hardware installation guide and the corresponding “Specifying the Interface Address on a SPA” topic in the platform-specific SPA software configuration guide for subslot information.
inst-info	Specifies the display of Instance Control Block information for the SPA.

region *region-number* **config** | **statistics**	Specifies the display of region-related TCAM manager information, with the following options:
	
	• **region** *region-number*-- Displays TCAM manager information, where:
	  • **region0**-- Specifies the destination MAC address TCAM region.
	  • **region1**-- Specifies the VLAN ID TCAM region.
	
	• **config** -- (Optional) Displays TCAM manager configuration information.
	
	• **statistics** -- (Optional) Displays TCAM manager statistical information.

rx-dest-mac | **rx-vlan** }{**alloc-mbussummary**] |**table**	Specifies the display of TCAM manager information related to the following areas: • **rx-dest-mac** --Destination MAC address filtering for received frames. • **rx-vlan** --VLAN filtering for received frames. • **alloc-mbus** **summary**]--Displays allocated Mask Block Unit (MBU) entry information related to the MAC or VLAN TCAM filters. There is no difference between the **alloc-mbus** and **alloc-mbussummary** form of the command. • **table** -- Displays table entries for the MAC or VLAN TCAM filters. **Note** The **label**and**free-mbussummary**] forms of the command are not supported on SPAs.

Command Default

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(19)S	This command was introduced.
12.2(20)S2	Thiscommand was integrated into Cisco IOS Release 12.2(20)S2 and support for the **subslot**, **rx-dest-mac**, and **rx-vlan** keywords were added for SPAs on the Cisco 7304 router.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **showtcam-mgrsubslot** command to display TCAM manager information for the destination MAC address and VLAN filter regions supported by the SPAs.

The TCAM manager allocates memory among the applications that it supports, in the form of regions. The SPAs support two TCAM regions, region 0 for destination MAC address filtering and region 1 for VLAN ID filtering of received frames.

Examples

The following examples provide sample output for several versions of the **showtcam-mgrsubslot** command for a 4-Port 10/100 Fast Ethernet SPA located in the top subslot (0) of the MSC that is installed in slot 4 on a Cisco 7304 router:

show tcam-mgr subslot inst-info Example

The following shows sample output from the **showtcam-mgrsubslotinst-info**command:

```
Router# show tcam-mgr subslot 4/0 inst-info
Instance Control Block Information :
CAM name                    =  SPA 4xFE/2xGE CAM2
Maximum key length          =  72 bits
TBU (TCAM Base Unit) length =  72 bits
V2M Ratio                   =  8
TCAM Size                   =  8192 TBUs
SRAM Size                   =  0 words
Start index of first VC     =  0
Label table size            =  0
```

show tcam-mgr subslot region Example

The following shows sample output from the **showtcam-mgrsubslotregion**command for the destination MAC address TCAM region (0) for the SPA:

```
Router# show tcam-mgr subslot 4/0 region 0
Region Configuration :
 Region ID                  =  0
 Region name                =  DA_FILTERING
 Fixed size                 =  no
```

```
 Region type (hash:mask    ) =  Partial_Order_Indep_Order_Dep_At_Bottom
 Application VMR V/M size    =  12
 Application VMR result size =  1
 Vc region size (percentage) =  50
Region Information :
 Region ID                  =   0
 Value cells size           =   4096
 Mask cells size            =   512
 MBUs size                  =   512
 Mask index start TBU       =   0
 Mask index end TBU         =   511
 First dynamic region       =   yes
 Last dynamic region        =   yes
 Size is fixed              =   yes
 Expansion unit MBUs        =   1
 Lower Limit, llimit_p      =   450A6CF0
 Upper Limit, ulimit_p      =   450AE4B4
 Lower limit pointer index  =   0
 Upper limit pointer index  =   511
 Lower next pointer index   =   0
 Upper next pointer index   =   4
 Lower free entries         =   1
 Upper free entries         =   507
 Bottom pointer index       =   510
 Free mask block units      =  508
 Region ID                   =  0
 Region expansion count      =  0
 Region Shifts             =  0
 Region expansion failures   =  0
 Invalid direction hits      =  0
 Invalid parameter hits      =  0
 No free entry failures      =  0
```

show tcam-mgr subslot region statistics Example

The following shows sample output from the **showtcam-mgrsubslotregionstatistics**command for the destination MAC address TCAM region (0) for the SPA:

```
Router# show tcam-mgr subslot 4/0 region 0 statistics
 Region ID                   =  0
 Region expansion count      =  0
 Region Shifts             =  0
 Region expansion failures   =  0
 Invalid direction hits      =  0
 Invalid parameter hits      =  0
 No free entry failures      =  0
```

show tcam-mgr subslot rx-dest-mac table Example

The following shows partial output from the **showtcam-mgrsubslotrx-dest-mactable**command:

```
Router# show tcam-mgr subslot 4/0 rx-dest-mac table
Dest mac filtering Table
-----------
 There are 15 entries in the table
 Entry# 1:
 Application ID              = 1
 Value                       =
                                0 0 0 0 0 4 0 0 0 0 0 0
```

```
 Mask                        =
                                0 0 0 0 0 C 0 0 0 0 0 0
 Result                      =
                                0
 Mask index                  = 511
 Mask Physical Address       = 4088
 Value cell index            = 7
 Value cell Physical address = 4095
 Allocation direction        = bottom
 Entry# 2:
 Application ID              = 1
 Value                       =
                                0 0 0 0 0 4 0 B0 64 FF 44 80
 Mask                        =
                                0 0 0 0 0 F FF FF FF FF FF FF
 Result                      =
                                4
 Mask index                  = 2
 Mask Physical Address       = 16
 Value cell index            = 1
 Value cell Physical address = 17
 Allocation direction        = no direction
 Entry# 3:
 Application ID              = 1
 Value                       =
                                0 0 0 0 0 4 FF FF FF FF FF FF
 Mask                        =
                                0 0 0 0 0 F FF FF FF FF FF FF
 Result                      =
                                4
 Mask index                  = 2
 Mask Physical Address       = 16
 Value cell index            = 2
 Value cell Physical address = 18
 Allocation direction        = no direction
.
.
.
```

show tcam-mgr subslot rx-vlan table Example

The following shows partial output from the **showtcam-mgrsubslotrx-vlantable**command:

```
Router# show tcam-mgr subslot 4/0 rx-vlan table
RX VLAN filtering Table
-----------
 There are 9 entries in the table
 Entry# 1:
 Application ID              = 2
 Value                       =
                                0 0 0 0 0 8 0 0 0 0 0 0
 Mask                        =
                                0 0 0 0 0 C 0 0 0 0 0 0
 Result                      =
                                0
 Mask index                  = 1023
 Mask Physical Address       = 8184
 Value cell index            = 7
 Value cell Physical address = 8191
 Allocation direction        = bottom
 Entry# 2:
```

```
 Application ID              = 2
 Value                       =
                                0 0 0 0 0 0 0 0 0 0 0 0
 Mask                        =
                                0 0 0 0 0 F 0 0 0 0 0 0
 Result                      =
                                4
 Mask index                  = 512
 Mask Physical Address       = 4096
 Value cell index            = 0
 Value cell Physical address = 4096
 Allocation direction        = top
.
.
.
```

show tcam-mgr subslot statisitics Example

The following shows sample output from the **showtcam-mgrsubslotstatisitics**command:

```
Router# show tcam-mgr subslot 4/0 statisitics
 Application entry alloc failures           =  0
 TCAM entry alloc failures                  =  0
 TCAM driver failures                       =  0
 TCAM API invalid parameters                =  0
 TCAM API application entry lookup failures  =  0
 TCAM API application entry mismatch failures=  0
 TCAM API label table occupied failures      =  0
 TCAM MGR free mbu vc failures              =  0
TCAM Mgr insertion/deletion time
  Insert  time: total:0.0000 num:0     avg:0.0000
    check dupl: total:0.0000 num:0     avg:0.0000
    alloc  mbu: total:0.0000 num:0     avg:0.0000
    queue appl: total:0.0000 num:0     avg:0.0000
    insert drv: total:0.0000 num:0     avg:0.0000
  Delete  time: total:0.0000 num:0     avg:0.0000
    delete drv: total:0.0000 num:0     avg:0.0000
    delete mbu: total:0.0000 num:0     avg:0.0000
    delete appl: total:0.0000 num:0     avg:0.0000
 Region ID                   =  0
 Region name                 =  DA_FILTERING
 Fixed size                  =  no
 Region type (hash:mask    ) =  Partial_Order_Indep_Order_Dep_At_Bottom
 Application VMR V/M size    =  12
 Application VMR result size =  1
 Vc region size (percentage) =  50
```

Related Commands

Command	Description
show controllers fastethernet	Displays Fast Ethernet interface information, transmission statistics and errors, and applicable MAC destination address and VLAN filtering tables.
show controllers gigabitethernet	Displays Gigabit Ethernet interface information, transmission statistics and errors, and applicable MAC destination address and VLAN filtering tables.

show tdm backplane

To display modem and PRI channel assignments with streams and channels on the modem side as assigned to the unit and channels on the PRI side of the time-division multiplexing (TDM) assignment, use the **showtdmbackplane**command in privileged EXEC mode.

show tdm backplane stream [*stream-number*]

Syntax Description

stream	Backplane stream in the range 0 to 7. There are 8 backplane "streams" on the TDM backplane for the Cisco AS5300 access server. Each stream runs at 2 MHz and has 32 channels (running at 64 Hz) on the Cisco AS5300 access server backplane hardware.
stream-number	(Optional) Actual number entered (either 0 to 7 or 0 to 15).

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(2)XD	This command was introduced.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **showtdmbackplane**command shows the status of the TDM backplane, related data structure values, and TDM chip memory settings. This commands is generally used only by a Cisco technical support representative during troubleshooting of data continuity problems.

Examples

The following example shows sample output for the **showtdmbackplane**command. When the **debugtdmdetail** command is executed, more detail is shown. The following examples are run with the **debugtdmdetail** command executed:

```
Router# show tdm backplane
Show BackPlane Connections
TDM Backplane Connection for Stream 0
     Modem (St/Ch)<->PRI (Unit/Ch)   xx/xx:Not Used ??/??:Unknown State
0  :  xx/xx<->xx/xx,  xx/xx<->xx/xx,  00/02<->00/30,  00/03<->03/10
4  :  00/04<->00/15,  00/05<->02/02,  00/06<->02/07,  00/07<->02/08
8  :  xx/xx<->xx/xx,  00/09<->03/11,  00/10<->02/09,  xx/xx<->xx/xx
12 :  00/12<->00/17,  00/13<->02/17,  00/14<->02/18,  00/15<->02/10
16 :  xx/xx<->xx/xx,  xx/xx<->xx/xx,  00/18<->00/19,  00/19<->02/19
20 :  00/20<->02/11,  xx/xx<->xx/xx,  xx/xx<->xx/xx,  00/23<->00/07
24 :  xx/xx<->xx/xx,  00/25<->00/01,  00/26<->00/20,  00/27<->02/20
28 :  xx/xx<->xx/xx,  00/29<->00/18,  xx/xx<->xx/xx,  xx/xx<->xx/xx

TDM Backplane Connection for Stream 1
     Modem (St/Ch)<->PRI (Unit/Ch)   xx/xx:Not Used ??/??:Unknown State
0  :  xx/xx<->xx/xx,  xx/xx<->xx/xx,  xx/xx<->xx/xx,  01/03<->03/09
```

```
4  :  01/04<->00/03,  01/05<->02/13,  xx/xx<->xx/xx,  xx/xx<->xx/xx
8  :  xx/xx<->xx/xx,  xx/xx<->xx/xx,  01/10<->02/14,  01/11<->00/04
12 :  01/12<->00/21,  xx/xx<->xx/xx,  01/14<->00/05,  xx/xx<->xx/xx
16 :  xx/xx<->xx/xx,  xx/xx<->xx/xx,  xx/xx<->xx/xx,  01/08<->02/12
20 :  01/20<->00/06,  01/09<->00/02,  xx/xx<->xx/xx,  xx/xx<->xx/xx
24 :  01/24<->03/01,  xx/xx<->xx/xx,  01/26<->02/15,  xx/xx<->xx/xx
28 :  01/28<->03/05,  xx/xx<->xx/xx,  xx/xx<->xx/xx,  xx/xx<->xx/xx
.
.
.
```

Related Commands

Command	Description
debug tdm detail	Displays debugging messages about TDM commands.
show tdm connections	Displays details about a specific TDM channel programmed on the Mitel chip.
show tdm data	Displays information about TDM bus connection memory on Cisco access servers.
show tdm detail	Displays information about the specified TDM device.
show tdm information	Displays TDM resources available for the specified TDM device.
show tdm pool	Displays information about the specified TDM pool.

show tdm connections

To display a snapshot of the time-division multiplexing (TDM) bus connection memory in a Cisco access server or to display information about the connection memory programmed on the Mitel TDM chip in a Cisco AS5800 access server, use the **showtdmconnections** command in privileged EXEC mode.

Standard Syntax

show tdm connections [{**motherboard** | **slot** *slot-nu mber*}]

Cisco AS5800 Access Server

show tdm connections {**motherboard stream** *stream-number* | **slot** *slot-number* **device** *device-number* **stream** *stream-number*}

Syntax Description

motherboard	(Optional) Displays connection memory for the TDM bus connections on the motherboard in the Cisco access server only. **Cisco AS5800 Access Server** The motherboard in the Cisco AS5800 access server has ethernet and serial interfaces, console port, and aux port. The motherboard has one TDM device (MT8980) for the Cisco 5300 access server.
slot *slot-number*	(Optional) Slot number. **Cisco AS5800 Access Server** There are three slots on the Cisco AS5800 access server. The range of the slots is from 0 to 2. A modem card or a trunk PRI card can be inserted into each slot. Each card in the slot has one or two TDM devices (either MT8980 or MT90820) on them.
stream	Device stream in the range 0 to 7. There are 8 backplane “streams” on the TDM backplane for the Cisco AS5800 access server. Each stream runs at 2 Mhz and has 32 channels (running at 64 Hz) on the Cisco AS5800 access server backplane hardware.
stream-number	Stream number (the range is from 0 to 7 or 0 to 15).
device	TDM device on the motherboard or slot cards. The range for the Cisco AS5800 access server is from 0 to 1. Each card has at least one TDM device (MT8980 or MT80920), and some of the slot cards have two devices (for example, the Octal PRI has two MT90820 TDM devices). The TDM device is also referred to as “TSI Chip Number” in the online help.
device-number	Valid range is from 0 to 1.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.0(3)T	This command was modified to include support for the Cisco AS5800 access server.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Cisco AS5800 Access Server

The **showtdmconnections**command shows the status of the TDM chip memory settings. This command is generally used only by a Cisco technical support representative during troubleshooting of data continuity problems.

Examples

Cisco AS5800 Access Server

The following example shows sample output for the **showtdmconnections**command. When the **debugtdmdetail** command is executed, more detail is shown. The following examples are run with the **debugtdmdetail** executed.

```
Router# show tdm connections slot 0
Slot 0 MT8980 TDM Device 0, Control Register = 0x1E, ODE Register = 0x01
Connection Memory for ST0:
Ch0:  0x00 0xE1, Ch1:  0x00 0xE2, Ch2:  0x01 0xDE, Ch3:  0x00 0x00
Ch4:  0x01 0xCF, Ch5:  0x00 0xE4, Ch6:  0x00 0xE5, Ch7:  0x00 0x00
Ch8:  0x00 0xEB, Ch9:  0x00 0xE6, Ch10: 0x00 0xE7, Ch11: 0x00 0x00
Ch12: 0x01 0xD1, Ch13: 0x00 0xE8, Ch14: 0x00 0x00, Ch15: 0x00 0xE9
Ch16: 0x00 0x00, Ch17: 0x00 0xD2, Ch18: 0x01 0xD3, Ch19: 0x00 0xEA
Ch20: 0x00 0xEB, Ch21: 0x00 0xC1, Ch22: 0x00 0xEC, Ch23: 0x01 0xC7
Ch24: 0x00 0xED, Ch25: 0x01 0xC1, Ch26: 0x01 0xD4, Ch27: 0x00 0xEE
Ch28: 0x00 0xE1, Ch29: 0x01 0xD2, Ch30: 0x00 0x00, Ch31: 0x00 0x00
Connection Memory for ST1:
Ch0:  0x00 0xEF, Ch1:  0x00 0xC2, Ch2:  0x00 0xED, Ch3:  0x00 0xF1
Ch4:  0x01 0xC3, Ch5:  0x00 0xF2, Ch6:  0x00 0xE2, Ch7:  0x00 0x00
Ch8:  0x00 0xF3, Ch9:  0x00 0xFF, Ch10: 0x00 0xF4, Ch11: 0x01 0xC4
Ch12: 0x01 0xD5, Ch13: 0x00 0xF5, Ch14: 0x01 0xC5, Ch15: 0x00 0xEE
Ch16: 0x00 0xF6, Ch17: 0x00 0xE3, Ch18: 0x00 0x00, Ch19: 0x00 0xF7
Ch20: 0x01 0xC6, Ch21: 0x01 0xC2, Ch22: 0x00 0xF8, Ch23: 0x00 0xE4
Ch24: 0x00 0xF9, Ch25: 0x00 0xC7, Ch26: 0x00 0x00, Ch27: 0x00 0xFA
Ch28: 0x00 0xFB, Ch29: 0x00 0xE5, Ch30: 0x00 0x00, Ch31: 0x00 0x00
```

Related Commands

Command	Description
debug tdm detail	Displays debugging messages about TDM commands.
show tdm data	Displays information about TDM bus connection memory on Cisco access servers.

show tdm data

To display a snapshot of the time-division multiplexing (TDM) bus data memory in a Cisco access server or to display data memory that is programmed on the Mitel TDM chip in a Cisco 5800 access server, use the **showtdmdata**command in privilegedEXEC mode.

Standard Syntax
show tdm data [{**motherboard** | **slot** *slot-number*}]

Cisco AS5800 Access Server
show tdm data {**motherboard stream** *stream-number* | **slot** *slot-number* **device** *device-number* **stream** *stream-number*}

Syntax Description

motherboard	(Optional) Displays bus data memory for the TDM bus connections on the motherboard in the Cisco access server only. **Cisco AS5800 Access Server** The motherboard on the Cisco AS5300 access server has the ethernet I/Fs, serial I/Fs, console port, and aux port. The motherboard has one TDM device (MT8980) for the Cisco AS5300 access server.
slot *slot-number*	(Optional) Slot number. **Cisco AS5800 Access Server** In addition to the motherboard, there are three slots on the Cisco AS5300 access server. The range of the slots is 0 to 2. A modem card or a trunk PRI card can be inserted in each slot. Each card in the slot has one or two TDM devices (either MT8980 or MT90820) on them.
stream	TDM device stream in the range 0 to 15. There are up to 16 streams on a TDM device (Mitel 90820). The TDM device is also known as the TSI chip. The help on the command (by typing **?**) indicates whether the stream is “Stream number within the TSI chip” or “Backplane Stream.”
stream-number	Stream number within the range of either 0 to 7 or 0 to 15.
device	TDM device on the motherboard, or slot cards. Valid range for the Cisco AS5300 access server is 0 to 1. Each card has at least one TDM device (MT8980 or MT80920), and the Octal PRI has two MT90820 TDM devices. Also referred to as TSI Chip Number in the help pages.
device-number	Valid range is from 0 to 1.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.0(3)T	This command was modified to include support for the Cisco AS5800 access server.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The data memory for all TDM bus connections in the access server is displayed if you do not specify a motherboard or slot.

Cisco AS5800 Access Server

The **showtdmdata**command shows the status of the TDM data structure values. This command is generally used only by a Cisco technical support representative during troubleshooting of data continuity problems.

Examples

The following is sample output for the **showtdmdata**command on a Cisco AS5800 access server. When the **debugtdmdetail** command is executed, more detail is shown. The following example is run with the **debugtdmdetail** executed:

```
Router# show tdm data
Motherboard MT8980 TDM Device 0, Control Register = 0x1F, ODE Register = 0xE1
Data Memory for ST0:
Ch0:  0xFF, Ch1:  0xFF, Ch2:  0x98, Ch3:  0x61
Ch4:  0x0C, Ch5:  0xE1, Ch6:  0x8D, Ch7:  0x86
Ch8:  0xFF, Ch9:  0xF3, Ch10: 0xE4, Ch11: 0xFF
Ch12: 0x51, Ch13: 0x02, Ch14: 0x18, Ch15: 0x14
Ch16: 0xFF, Ch17: 0xFF, Ch18: 0x05, Ch19: 0xC7
Ch20: 0x00, Ch21: 0xFF, Ch22: 0xFF, Ch23: 0x98
Ch24: 0xFF, Ch25: 0x15, Ch26: 0x5C, Ch27: 0x15
Ch28: 0xFF, Ch29: 0x80, Ch30: 0xFF, Ch31: 0xFF
Data Memory for ST1:
Ch0:  0xFF, Ch1:  0xFF, Ch2:  0xFF, Ch3:  0x62
Ch4:  0x94, Ch5:  0x88, Ch6:  0xFF, Ch7:  0xFF
Ch8:  0xFF, Ch9:  0xFF, Ch10: 0xFB, Ch11: 0x91
Ch12: 0xF7, Ch13: 0xFF, Ch14: 0x96, Ch15: 0xFF
Ch16: 0xFF, Ch17: 0xFF, Ch18: 0xFF, Ch19: 0x94
Ch20: 0x8F, Ch21: 0x95, Ch22: 0xFF, Ch23: 0xFF
Ch24: 0xE2, Ch25: 0xFF, Ch26: 0xD3, Ch27: 0xFF
Ch28: 0x87, Ch29: 0xFF, Ch30: 0xFF, Ch31: 0xFF
Data Memory for ST2:
.
.
.
```

Related Commands

Command	Description
debug tdm detail	Displays debugging messages about TDM commands.
show tdm connections	Displays details about a specific TDM channel programmed on the Mitel chip.

show tdm detail

To display details about a specific time-division mulltiplexing (TDM) channel programmed on the Mitel chip, use the **showtdmdetail**command in privileged EXEC mode.

show tdm detail *slot-number*/*device-number* *source-stream-number*/*source-channel-number*

Syntax Description

slot-number	There are three slots on the Cisco AS5300 access server. A modem card or a trunk Primary Rate Interface (PRI) card can be inserted in each slot. Each card has one or two TDM devices (either MT8980 or MT90820) on it. The valid range is from 0 to 2.
device-number	TDM device on the motherboard or slot cards. Each card has at least one TDM device (MT8980 or MT80920), and the Octal PRI has two MT90820 TDM devices. Also referred to a TSI Chip Number in the online help. The valid values are 0 to 1.
source-stream-number	Source stream number from the TDM device. The valid range is from 0 to 15.
source-channel-number	Source channel from the TDM device stream. The valid range is from 0 to 31.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.0(2)XD	This command was introduced.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

The **showtdmdetail**command shows the status of the TDM backplane, related data structure values, and TDM chip memory settings. This command is generally used only by a Cisco technical support representative during troubleshooting of data continuity problems.

This command indicates connection memory and map, data memory, and whether the channel is enabled or disabled. Specify the slot, TDM device, TDM stream, and TDM channel to view the appropriate details.

Examples

The following is sample output from the **showtdmdetail**command. When the **debugtdmdetail**command is executed, more detail is shown. The following example was run with the **debugtdmdetail** command executed. The fields are self-explanatory.

```
Router# show tdm detail 0/0 1/2
Show Detail TDM device info: slot 0 unit 0
ODE Register: 0x0001
```

```
Connection Memory: 0x00ED, Output is Disable
Connection Map: STi7 CHi13 ----> STo1 CHo2
Data Memory: 0x00FF
```

Related Commands

Command	Description
debug tdm detail	Displays debugging messages about TDM commands.
show tdm backplane	Displays modem and PRI channel assignments with streams and channels on the modem side as assigned to the unit and channels on the PRI side of the TDM assignment.
show tdm connections	Displays details about a specific TDM channel programmed on the Mitel chip.
show tdm data	Displays information about TDM bus connection memory on Cisco access servers.
show tdm information	Displays TDM resources available for the specified TDM device.
show tdm pool	Displays information about the specified TDM pool.

show tdm information

To display information about the specified time-division multiplexing (TDM) device, use the **showtdminformation**command in privileged EXEC mode.

show tdm information {**motherboard** | **slot** *slot-number* **device** *device-number*}

Syntax Description

motherboard	Motherboard on the Cisco AS5300 access server has the Ethernet I/Fs, serial I/Fs, console port, and aux port. The motherboard has one TDM device (MT8980) for the Cisco AS5300 access server.
slot	There are three slots on the Cisco AS5300 access server. The range of the slots is 0 to 2. A modem card or a trunk PRI card can be inserted in each slot. Each card has one or two TDM devices (either MT8980 or MT90820) on it.
slot-number	Slot number. Valid range is from 0 to 2.
device	TDM device on the motherboard or slot cards. The valid range is from 0 to 1. Each card has at least one TDM device (MT8980 or MT80920), and the Octal PRI has two MT90820 TDM devices. Also referred to as TSI Chip Number in the online help.
device-number	Device number. Valid range is from 0 to 1.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(2)XD	This command was introduced.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **showtdminformation**command shows the status of the TDM backplane, related data structure values, and TDM chip memory settings. This command is generally used only by a Cisco technical support representative during troubleshooting of data continuity problems.

This command displays the register base address, device type, and capabilities on a per-slot basis.

Examples

The following example shows sample output for the **showtdminformation**command. When the **debugtdmdetail** command is executed, more detail is shown. The following example is run with the **debugtdmdetail** command executed:

```
Router# show tdm information motherboard
TDM Slot Info display for Motherboard:
  Slot Info ptr @0x610D39C0  Feature info ptr @0x60B737E8
  Feature board is MOTHERBOARD, NIM ID: 0x30
```

```
  TSI device is MT8980, 1 on this board. Each TSI device supports 0 DS1s
  First TSI device is at offset: 0x100
  TSI device 0, register base 0x3E801100
    TDM Device Info ptr @0x611AA3EC for slot -1
    TSI device Info ptr @0x60FCC0BC   memory size = 0x100
      This device supports 8 streams with 32 channels per stream
TDM Information display for slot 0:
  Slot Info ptr @0x610D39E4  Feature info ptr @0x60B73818
  Feature board is E1 Quad PRI, NIM ID: 0x43
  TSI device is MT8980, 2 on this board. Each TSI device supports 2 DS1s
  First TSI device is at offset: 0x100, Second TSI device is at Offset: 0x200
  HDLC   Streams start at 4
  Framer Streams start at 6
  TSI device 0, register base 0x3C400100
    TDM Device Info ptr @0x61222054 for slot 0
    TSI device Info ptr @0x60FCC0BC   memory size = 0x100
      This device supports 8 streams with 32 channels per stream
  TSI device 1, register base 0x3C400200
    TDM Device Info ptr @0x61222098 for slot 0
    TSI device Info ptr @0x60FCC0BC   memory size = 0x100
      This device supports 8 streams with 32 channels per stream
TDM Information display for slot 1:
  Slot Info ptr @0x610D3A08  Feature info ptr @0x60B738A8
  Feature board is High Density Modems, NIM ID: 0x47
  TSI device is MT8980, 1 on this board. Each TSI device supports 0 DS1s
  First TSI device is at offset: 0x100
  TSI device 0, register base 0x3C500100
    TDM Device Info ptr @0x612F1B80 for slot 1
    TSI device Info ptr @0x60FCC0BC   memory size = 0x100
      This device supports 8 streams with 32 channels per stream
TDM Information display for slot 2:
  Slot Info ptr @0x610D3A2C  Feature info ptr @0x60B738A8
  Feature board is High Density Modems, NIM ID: 0x47
  TSI device is MT8980, 1 on this board. Each TSI device supports 0 DS1s
  First TSI device is at offset: 0x100
  TSI device 0, register base 0x3C600100
    TDM Device Info ptr @0x613A6F60 for slot 2
    TSI device Info ptr @0x60FCC0BC   memory size = 0x100
      This device supports 8 streams with 32 channels per stream
```

Related Commands

Command	Description
debug tdm detail	Displays debugging messages about TDM commands.
show tdm backplane	Displays modem and PRI channel assignments with streams and channels on the modem side as assigned to the unit and channels on the PRI side of the TDM assignment.
show tdm connections	Displays details about a specific TDM channel programmed on the Mitel chip.
show tdm data	Displays information about TDM bus connection memory on Cisco access servers.
show tdm detail	Displays information about the specified TDM device.
show tdm pool	Displays information about the specified TDM pool.

show tdm pool

To display time-division multiplexing (TDM) resources available for a TDM device, use the **showtdmpool**command in privileged EXEC mode.

show tdm pool [**slot** *slot-number*]

Syntax Description

slot	(Optional) There are three slots on the Cisco AS5300 access server with a range of 0 to 2. A modem card or a trunk PRI card can be inserted in each slot. Each card has one or two TDM devices (either MT8980 or MT90820) on it.
slot-number	(Optional) Slot number. Valid range is from 0 to 2 for the Cisco AS5300 access server.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(2)XD	This command was introduced.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **showtdmpool**command shows the status of the TDM backplane, related data structure values, and TDM chip memory settings. This command is generally used only by a Cisco technical support representative during troubleshooting of data continuity problems.

This command displays TDM groups, where group 0 is streams 0 to 3 and group 1 is streams 4 to 7. It also displays register address and capabilities on a per-slot basis.

Examples

The following example shows sample output for the **showtdmpool**command. When the **debugtdmdetail** command is executed, more detail is shown. The following example was run with the **debugtdmdetail** command executed:

```
Router# show tdm pool
Dynamic Backplane Timeslot Pool:
 Grp ST Ttl/Free Req(Cur/Ttl/Fail)       Queues(Free/Used)      Pool Ptr
  0 0-3  120 60     60  361      0       0x61077E28  0x61077E28  0x61077E20
  1 4-7  0   0      0   0        0       0x61077E38  0x61077E28  0x61077E24
```

Related Commands

Command	Description
debug tdm detail	Displays debugging messages about TDM commands.

Command	Description
show tdm backplane	Displays modem and PRI channel assignments with streams and channels on the modem side as assigned to the unit and channels on the PRI side of the TDM assignment.
show tdm connections	Displays details about a specific TDM channel programmed on the Mitel chip.
show tdm data	Displays information about TDM bus connection memory on Cisco access servers.
show tdm detail	Displays information about the specified TDM device.
show tdm information	Displays TDM resources available for the specified TDM device.

show tunnel interface

To display detailed information for a specified tunnel interface or for all tunnel interfaces, use the **show tunnel interface** command in user EXEC or privileged EXEC mode.

show tunnel interface [{**tunnel** *tunnel-number*}]

Syntax Description

tunnel *tunnel-number*	(Optional) Specifies a tunnel interface identifier.

Command Default

Information about all tunnels on a device is displayed.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.6S	This command was introduced.
15.1(1)SY	This command was modified. The output was enhanced to display information about how a tunnel is created.

Examples

The following is sample output from the **show tunnel interface tunnel** command for a specific tunnel:

```
Device# show tunnel interface tunnel 1

Tunnel1
   Mode:PIM/IPv4, Destination 127.0.102.1, Source Ethernet0/0
   IP transport: output interface unknown next hop 127.0.102.1
   Application ID 3: unspecified
   Tunnel Subblocks:
      src-track:
         Tunnel1 source tracking subblock associated with Ethernet0/0
          Set of tunnels with source Ethernet0/0, 3 members (includes iterators)
, on interface <OK>
   Linestate - current down
   Internal linestate - current down, evaluated down - interface not up
   Tunnel Source Flags: Local  Remote

Tunnel1 is up (if_number 30) ['1]
  Corresponding hwidb fast_if_number 30
  Corresponding hwidb firstsw->if_number 30
  Internet address is 0.0.0.0/0
  Unnumbered interface. Using address of Ethernet0/0 (127.0.102.2)
  ICMP redirects are never sent
  Per packet load-sharing is disabled
  IP unicast RPF check is disabled
  Suppressed input features: MCI Check
  Suppressed output features: IP Post Routing Processing
  Suppressed post encapsulation features: MTU Processing, IP Protocol Output Cou
nter, IP Sendself Check
  IP policy routing is disabled
```

```
  BGP based policy accounting on input is disabled
  BGP based policy accounting on output is disabled
  Interface is marked as point to point interface
  Interface is marked as tunnel interface
  Hardware idb is Tunnel1
  Fast switching type 14, interface type 0
  IP CEF switching enabled
  IP prefix lookup IPv4 mtrie generic
  Flags 0x46049, hardware flags 0x8
  Input fast flags 0x0, Output fast flags 0x0
  ifindex 28(6) ['1]
  Slot unknown Slot unit -1 VC -1
  IP MTU 1472
  Real output interface is Ethernet0/0
 Switching statistics:
  Input: 0 packets, 0 bytes
  Output: 0 packets, 0 bytes
 Subblocks:
  Tunnel1: mode 25, submode 0
  fibhwidb if_number:28 fibidb if_number 30
  Tunnel source UNKNOWN, destination 124.0.102.1
  Tunnel protocol/transport, PIM/IPv4 key disabled
  Tunnel flags: 0x2000480 flags_private 0x0
  Enable sequencing:no, Enable checksum: no
  Carry ipso:no, Fast capable:no
  Tableid: 0 Appid:3
  Tunnel Source Flags:  Remote
  IPv4: Internet address is 0.0.0.0/0
        Unnumbered interface. Using address of Ethernet0/0 (127.0.102.2)
        Broadcast address 255.255.255.255
        Per packet load-sharing is disabled
        ICMP redirects are never sent
        ICMP unreachables are always sent
        IP MTU 1472
  MFIB IPv4 @01C0CD28 wire=01C0F528
        fixup:  UNUSED   (0)
```

The following is sample output from the **show tunnel interface** command:

```
Device# show tunnel interface

Tunnel0
   Mode:multi-GRE/IP, Destination UNKNOWN, Source GigabitEthernet1/1
   Application ID 2: L3VPN : profile : TEST
   Tunnel Subblocks:
      src-track:
         Tunnel0 source tracking subblock associated with GigabitEthernet1/1
          Set of tunnels with source GigabitEthernet1/1, 2 members (includes ite
rators), on interface <OK>
   Linestate - current up
   Internal linestate - current up, evaluated up
   Tunnel Source Flags: Local
   OCE: IP tunnel decap
   Provider: interface Tu0, prot 47
     Performs protocol check [47]
     Protocol Handler: GRE: opt 0x0
       ptype: ipv4 [ipv4 dispatcher: punt]
       ptype: ipv6 [ipv6 dispatcher: punt]
       ptype: mpls [mpls dispatcher: from if Tu0]
Tunnel20
   Mode:GRE/IP, Destination 127.0.38.1, Source GigabitEthernet1/1
   IP transport: output interface GigabitEthernet1/1 next hop 127.0.38.1
   Application ID 1: unspecified
```

```
   Tunnel Subblocks:
      src-track:
         Tunnel20 source tracking subblock associated with GigabitEthernet1/1
          Set of tunnels with source GigabitEthernet1/1, 2 members (includes ite
rators), on interface <OK>
   Linestate - current up
   Internal linestate - current up, evaluated up
   Tunnel Source Flags: Local
   OCE: IP tunnel decap
   Provider: interface Tu20, prot 47
     Performs protocol check [47]
     Protocol Handler: GRE: opt 0x0
       ptype: ipv4 [ipv4 dispatcher: punt]
       ptype: ipv6 [ipv6 dispatcher: punt]
       ptype: mpls [mpls dispatcher: drop]
There are 0 tunnels running over the EON IP protocol
There are 0 tunnels running over the IPinIP protocol
There are 0 tunnels running over the NOSIP protocol
There are 0 tunnels running over the IPv6inIP protocol
```

The table below describes the significant fields shown in the displays.

Table 273: show tunnel interface Field Descriptions

Field	Description
Mode	Tunnel encapsulation method. For example, GRE, IP in IP, IPv6 in IP.
Destination	Destination address of the tunnel packets. This field is relevant for point-to-point tunnels only.
Source	Source of packets in a tunnel.
IP transport	Destination of IP packets.
Application ID	Application that created the tunnel. For example,L3VPN, PIM, and generic applications that use a tunnel created using the CLI.
Tunnel Subblocks	Subset of tunnel information that is accessible through a Forwarding Information Base (FIB) Hardware Interface Descriptor Block (HWIDB) subblock.
src-track	Indicates the interface on which source tracking needs to be enabled in case an attack is suspected on a tunnel. Also indicates the number of tunnels associated with this interface.
Linestate	Indicates the state of the interface.
Tunnel Source Flags	Flag that indicates the set of sources for a tunnel. The value of this flag can be as follows: • Local—Indicates that the tunnel was created locally by an application. Tunnels on an active Route Processor (RP) have only a local source set. • Remote—Indicates that the tunnel was created on receipt of an External Data Representation (XDR) message. Tunnels on a standby RP always have a remote source set. The tunnels may also have a local source set if the application created a tunnel on the standby.

Field	Description
Corresponding hwidb	Corresponding HWIDB. This is the system-wide representation of an interface. There is one HWIDB per interface.
OCE	Output chain elements (OCEs) applied to tunnel packets after an adjacency. This is an object that is used to decapsulate traffic received on a tunnel and dispatch the payload. There is only one decapsulation OCE associated with a tunnel.
Provider	IP protocol type number of the tunneling protocol used. For example, GRE packets that are encapsulated within IP use IP protocol type 47.
ptype	Each tunnel endpoint can receive packets of different payload types. Each payload type has an adjacency associated with it. The payload type can include the Layer 2 next-hop address to which the tunnel packet has to be forwarded or special adjacency type information such as Drop (drop the packets) or Punt (forward the packets to a higher switching layer such as fast switching).
Switching statistics	Number of packets that have been received by the tunnel, forwarded through the tunnel, or dropped by the tunnel.
Subblocks	Subset of tunnel information that is accessible via a FIB HWIDB subblock.
Enable sequencing	Indicates whether sequencing of packets is enabled.
Carry ipso	Indicates whether IP Security Option (IPSO) or Commercial IP Security Option (CIPSO) labels are acquired from parent.
Fast capable	Indicates whether fast tunneling is possible.
Tableid	Indicates the table ID associated with the transport Virtual routing and forwarding (VRF).
Appid	Tunnel application identity.

Related Commands

Command	Description
show cef interface	Displays detailed Cisco Express Forwarding information for a specified interface or for all interfaces.

show tunnel keys-database tunnel

To display all transmit and receive generic routing encapsulation (GRE) key pairs associated with traffic flows in a tunnel, use the **show tunnel keys-database tunnel** command in privileged EXEC mode.

show tunnel keys-database tunnel *tunnel-number*

Syntax Description

tunnel-number	Tunnel number. The range is from 0 to 2147483647.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Usage Guidelines

A key can be optionally added to a GRE tunnel and used to identify a traffic flow within the tunnel, as defined in RFC 2890, *Key and Sequence Number Extensions to GRE*.

GRE keys can be used in various ways in a network, and one such use case is in the Proxy Mobile IPv6 (PMIPv6) application. To facilitate seamless movement of mobile users from one access network to another, PMIPv6 as described in RFC 5213, *Proxy Mobile IPv6*, defines network-based mobility protocols that allow mobile users to communicate without disruption while roaming. The solution requires IP tunneling of packets of mobile nodes from a Mobile Access Gateway (MAG) to a Local Mobility Anchor (LMA). A mobile node is an IP host or a device whose mobility is managed by the network. The LMA is the home agent for a mobile node in a PMIPv6 domain. The MAG is an access router function that manages mobility-related signaling for a mobile node, tracks the mobile node's movements, and signals the LMA. RFC 5845, *GRE Key Option for Proxy Mobile IPv6* further explains the scenario in which multiple GRE keys can be used to differentiate packets of a specific mobile session in a tunnel between an LMA and a MAG.

Tunnel endpoints are added by applications. For example, Next Hop Resolution Protocol (NHRP) adds the endpoint for Dynamic Multipoint Virtual Private Network (DMVPN) application. An endpoint is associated with a transport address and in many cases with an overlay address. The transport address corresponds to the egress point of a tunnel, which is where the tunnel terminates, and an overlay address can be any address reachable on or beyond the tunnel's egress point in the network.

Applications can add an endpoint with an overlay address and a corresponding transport address. In case applications do not need an overlay address or just need to forward packets to an endpoint based on a policy, they can add an endpoint with just a transport address.

In the context of PMIPv6, the overlay address corresponds to the mobile node address, and the transport address corresponds to either the Proxy Care-of Address (global address configured on the egress interface of the MAG) or the LMA address depending on where the endpoint is being added. When an endpoint is added on an LMA, the transport address is the Proxy Care-of Address of the MAG. When an endpoint is added on the MAG, the transport address is the LMA address.

The tunnel maintains a GRE key database, that is accessed by the forwarding plane using a receive GRE key that is unique for a tunnel. The receive GRE key database is populated on the request of an application when the application is associated with a tunnel. The receive key database also has other data such as the list of operations to be done before forwarding the payload. One of these operations is the setting of virtual routing and forwarding (VRF)-ID.

VRF-ID is an optional parameter that is used by applications to set the egress of the tunnel before forwarding packets. This can be used in case there are overlapping mobile node IP addresses belonging to different VRFs. At the egress of a tunnel, the forwarding plane can look up the GRE key database based on the received GRE Key and get the corresponding VRF-ID. If the VRF-ID is not set, the forwarding plane sets the VRF-ID based on the VRF of the tunnel interface.

Examples

The following is sample output from **show tunnel keys-database tunnel 0**, which shows all transmit and receive GRE key pairs associated with various traffic flows in a tunnel:

```
Device# show tunnel keys-database tunnel 0

Remote address 10.1.1.2, RefCount 2
Transmit Key 16, Receive Key 15, Association 1.1.1.2
Connection-ID 16, VRF-Override enabled, VRF-ID 65535
Transmit Key 161, Receive Key 151, Association 1.1.1.3
Connection-ID 161, VRF-Override enabled, VRF-ID 65535
```

The table below describes the significant fields shown in the display.

Table 274: show tunnel keys-database tunnel Field Descriptions

Field	Description
Remote address	Overlay address or a remote IPv4 or IPv6 address, reachable beyond the tunnel endpoint in the network.
RefCount	Reference count used for debugging.
Transmit Key	Transmit key associated with a flow.
Receive Key	Receive key associated with a flow.
Association	Associated flow identifier. For example, IP address in the payload.
Connection-ID	Locally stored connection identifier used for key insertion in a packet.
VRF-Override enabled	Flag that indicates which VRF to forward the received packets. If the flag is enabled, the received packets are forwarded to the VRF with a given VRF-ID. If the flag is disabled, the received packets are forwarded to the tunnel interface VRF.
VRF-ID	VRF identifier associated with a key.

show top counters interface report

To display TopN reports and information, use the **showtopcountersinterfacereport** command in user EXEC or privileged EXEC mode.

show top counters interface report [*number*]

Syntax Description

number	(Optional) Number of the report to be displayed; valid values are from 1 to 5.

Command Default

This command has no default settings.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported on Ethernet, Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet ports only. LAN ports on the OSMs are also supported.

When you enter a TopN request, a round of polling is performed, the counters for all the applicable ports in the Cisco 7600 series router are read, and the information is saved. The TopN process then sleeps for the specified interval. After wakeup, another round of polling is performed and the counter information from the ports is read. The difference between the two sets of data is stored. The ports are then sorted, the ports choose from one of the seven types of statistics information, and a TopN report is generated.

The port statistics will not be displayed in the following cases:

- If a port is not present during the first poll.
- If a port is not present during the second poll.
- If a port's speed or duplex changes during the polling interval.
- If a port's type changes from Layer 2 to Layer 3 or Layer 3 to Layer 2 during the polling interval.

Note For the report display format, due to the 80 characters per line limitation, only 10 spaces are reserved for the Tx/Rx-okts, Tx/Rx-bcst, and Tx/Rx-mcst columns. When these columns are larger than 10 digits, the display wraps around to the next line.

When you start the TopN processes from a Telnet session and the Telnet session is terminated before the TopN processes are completed, all the backgound TopN processes continue and generate the TopN reports, but the foreground TopN processes are terminated once the Telnet session is terminated.

When the TopN report is being generated against a large number of ports (for example, 13 slot x 96 ports/slot) in a very short interval (10 seconds), the actual interval time between the first and second polling may be longer than the specified interval time because polling takes time.

Examples

This example shows how to display TopN reports and information:

```
Router# show top counters interface report
Id Start Time                   Int N   Sort-By   Status  Owner
-- ---------------------------- --- --- --------- ------- ----------------------
1  08:18:25 UTC Tue Nov 23 2004 76  20  util      done    console
2  08:19:54 UTC Tue Nov 23 2004 76  20  util      done    console
3  08:21:34 UTC Tue Nov 23 2004 76  20  util      done    console
4  08:26:50 UTC Tue Nov 23 2004 90  20  util      done    bambam onvty0 (9.10.69.13)
Router#
```

This example shows how to display TopN reports and information for a specific report:

```
Router# show top counters interface report
 1
Started By        : console
Start Time        : 08:18:25 UTC Tue Nov 23 2004
End Time          : 08:19:42 UTC Tue Nov 23 2004
Port Type         : All
Sort By           : util
Interval          : 76 seconds
Port    Band  Util Bytes       Packets     Broadcast  Multicast  In-  Buf-
        width      (Tx + Rx)   (Tx + Rx)   (Tx + Rx)  (Tx + Rx)  err  ovflw
------- ----- ---- ----------- ----------- ---------- ---------- ---- -----
Fa2/5   100   50   726047564   11344488    11344487   1          0    0
Fa2/48  100   35   508018905   7937789     0          43         0    0
Fa2/46  100   25   362860697   5669693     0          43         0    0
Fa2/47  100   22   323852889   4762539     4762495    43         0    0
Fa2/6   100   15   217815835   3403372     0          39         21   0
Fa2/44  100   10   145146009   2267900     0          43         0    0
Gi4/15  1000  0    0           0           0          0          0    0
Gi4/14  1000  0    0           0           0          0          0    0
Gi4/13  1000  0    0           0           0          0          0    0
Gi4/12  1000  0    0           0           0          0          0    0
Gi4/11  1000  0    0           0           0          0          0    0
Gi4/10  1000  0    0           0           0          0          0    0
Gi4/9   1000  0    0           0           0          0          0    0
Gi4/8   1000  0    776         2           0          2          0    0
Gi4/7   1000  0    0           0           0          0          0    0
Gi4/6   1000  0    0           0           0          0          0    0
Gi4/5   1000  0    0           0           0          0          0    0
Gi4/4   1000  0    0           0           0          0          0    0
Gi4/3   1000  0    776         2           0          2          0    0
Gi4/2   1000  0    0           0           0          0          0    0
Router#
```

This example shows the display if you request a TopN report that is still in pending status:

```
Router# show top counters interface report
 4
Id   Start time          Int N   Sort-by     Status   Owner (type/machine/user)
---  ------------------- --- --- ---------- -------- -------------------------
  4  1/24/2004,11:34:26  30  20  In-Errors  pending  Console//
Router#
```

Related Commands

Command	Description
clear top counters interface report	Clears the TopN reports.
collect top counters interface	Lists the TopN processes and specific TopN reports.

show ucse imc download progress

To display the status of the CIMC firmware download, use the **show ucse imc download progress** command in EXEC mode.

show ucse *slot* **imc download progress**

Syntax Description

slot	Router slot number in which the Cisco E-Series Server is installed.

Command Modes

Privileged EXEC mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

When the CIMC firmware is downloading, this command displays the percentage complete. After the download is complete, this command displays the last known download status.

Examples

The following examples show how to display the status of the CIMC firmware download:

```
Router# show ucse 2 imc download progress

Download is in progress (1% - 9894k/679M - 1kB/s)
Router# show ucse 2 imc download progress

No Download is not currently in process
Last download status: Downloaded successfully : ubuntu-server.iso
```

show ucse imc files

To display the CIMC installable images that are available on the local file system, use the **show ucse imc files** command in EXEC mode.

show ucse *slot* **imc files**

Syntax Description

slot	Router slot number in which the Cisco E-Series Server is installed.

Command Modes

Privileged EXEC mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

Use this command to determine which images can be used to boot the server, or which files can be deleted to free up space.

Examples

The following example shows how to display the CIMC firmware files:

```
Router# show ucse 2 imc files

Directory of UCSE slot 2 imc filesystem
 -rw-  1697952   May 5 2010 16:55:04 +00.00 debian.iso
```

show ucse server boot

To display the device types from which the Cisco E-Series Server can boot, the order in which the boot is attempted, or the progress of boot initialization, use the **show ucse server boot** command from EXEC mode.

show ucse *slot* **server boot** [{**devices** | **order** | **progress**}]

Syntax Description

slot	Router slot number in which the Cisco E-Series Server is installed.
devices	The device types available to the module from which the Cisco E-Series Server can boot. It can be one of the following: • HDD—Hard disk drive • FDD—Floppy disk drive • CDROM—Bootable CD-ROM • PXE—PXE boot • EFI—Extensible Firmware Interface
order	The current order in which the boot configuration will be attempted.
progress	The status of the image boot and image download.

Command Modes

Privileged EXEC mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

Use the output of this command to see the boot options.

Examples

The following example displays the list of all devices that can be used to boot the module:

```
Router# show ucse 1 server boot devices

PXE
FDD
HDD:HDD3
HDD:RAID-MD0
HDD:USB-FF5D6CC3DAA67F12-1
CDROM:USB-CD
```

The following example shows how to display the boot order:

```
Router# show ucse 1 server boot order

Currently booted from CDROM:USB-CD
Boot order:
```

```
1) PXE
2) CDROM:USB-CD
3) FDD
4) HDD:RAID-MD0
```

show ucse server erase device status

To display the status of devices that have been erased, use the **show ucs server erase device status** command in EXEC mode.

show ucse *slot* **server erase device status**

Syntax Description

slot	Router slot number in which the Cisco E-Series Server is installed.

Command Modes

Privileged EXEC mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

Use this command after you have erased HDDs using the **ucse** *slot* **server erase device hh [all | use***device_list***]**command.

Examples

The following example shows how to display the details after erasing HDDs:

```
Router# ucse 2 server erase device hdd use hdd2

You are about to erase all data on the selected hard drives.
Proceed with drive erasure? y

Erasing HDD2 started
Router#
Router# show ucse 2 server erase device status

HDD2 erased 0%
```

show ucse server raid level

To display the current RAID configuration, use the **show ucse server raid level** command in EXEC mode.

show ucse *slot* **server raid level**

Syntax Description

slot	Router slot number in which the Cisco E-Series Server is installed.

Command Modes

Privileged EXEC mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

Use this command after you have configured the RAID levels by using the **ucse** *slot* **server raid level** {**0** | **1** | **5** | **NONE**} [**use** *HDD_list*] command.

Examples

The following example shows how to display RAID details:

```
Router# ucse 2 server raid level 1

You are about to change RAID configuration.
It will destroy all data on the hard drives.

Are you sure [y/n] y
RAID reconfigured
Router# show ucse 2 server raid level

RAID 0 (Ctrl:SLOT-5 ID:0 Size:1905440 MB State:Optimal)
        HDD1 :              953869 MB online (0 errors)
      HDD255 :              953869 MB online (0 errors)
HDDs not in the RAID:
        HDD2 :              286102 MB system (0 errors)
```

show upgrade file

The show upgrade file command is replaced by the **show upgrade fpd file** command. See the **show upgrade fpd file** command for more information.

show upgrade fpd file

To display the contents of an FPD image package file, enter the **showupgradefpdfile** command in privileged EXEC mode.

show upgrade fpd file *file-url* [**detail**]

Syntax Description

file-url	Specifies the location of the FPD image package file, beginning with the location or type of storage device (examples include **disk0**, **slot0**, **tftp**, or **ftp**) and followed by the path to the FPD image package file.
detail	(Optional) Displays detailed information about the contents of the FPD image package file. This option is intended for use by Cisco customer support personnel only.

Command Default

No default behavior or values

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(20)S6	This command was introduced and replaced the **showupgradefile** command on the Cisco 7304 router.
12.2(25)S3	The output of the **showupgradefpdfile***file-url* command was changed to display only brief versioning information. The output generated from this command in previous Cisco IOS releases can still be generated in this release by entering the **showupgradefpd***file-url***detail** command. The **detail** option is also new in this release.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(4)XD	This command was integrated into Cisco IOS Release 12.4(4)XD.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.

Usage Guidelines

This command provides information related to the FPD image package file. Most of the information in this command output is useful for Cisco customer support purposes only.

In Cisco IOS Releases 12.2(20)S2 through 12.2(20)S5, the output generated by entering this command can be generated by entering the **showupgradefile** command.

For more information about FPD upgrades on SPA interface processors (SIPs) and shared port adapters (SPAs), see the Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide.

Examples

Cisco 7200 VXR

The following example shows that the router is able to generate FPD image package information for the FPD image package on the TFTP server:

```
Router# show upgrade fpd file tftp://mytftpserver/myname/myfpdpkg/c7200-fpd-pkg.124-4.XD.pkg
Loading /auto/tftpboot-users/jsmith/c7200-fpd-pkg.124-4.XD.pkg from 223.255.254.254 (via
GigabitEthernet0/1):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 1419264 bytes]
Cisco Field Programmable Device Image Package for IOS
C7200 FPD Image Package (c7200-fpd-pkg.124-4.XD.pkg), Version 12.4(20060105:195420)
Copyright (c) 2005-2006 by cisco Systems, Inc.
Built Thu 05-Jan-2006 11:54 by abcdef
=============================== ================================================
                                        Bundled FPD Image Version Matrix
                                ================================================
                                                                      Min. Req.
Supported Card Types            ID  Image Name                Version  H/W Ver.
=============================== == ========================= ========= =========
NPEG2 IOFPGA                     1 NPEG2 IOFPGA                 0.7       0.0
------------------------------- -- ------------------------- --------- ---------
VSA                              1 VSA                          0.8       0.0
=============================== ================================================
```

Cisco 7304

The output in the following example displays information about the FPD image package file stored in the disk0: Flash card memory:

```
Router# show upgrade fpd file disk0:spa-fpd.122-20.S6.pkg
% Extracting compressed bundle spa_4fe2ge-fpd.bndl.zip ...
Content for the "spa_4fe2ge-fpd.bndl" bundle file:
                     Bundle Name:4xFE/2xGE SPA FPD Bundle
                  Bundle Version:0.5
       Number of Supported Cards:2
          Supported Card Type(s):SPA-4FE-7304 (0x435)
                                  SPA-2GE-7304 (0x436)
    Bundle Header Format Version:4
            Bundle Header Length:128 bytes
              Bundle Data Length:4951592 bytes
             Bundle Magic Number:0xC5C0FBC0
               Bundle 32-Bit CRC:0x3B53C5C0
               Bundle Build Date:10/12/2004 (MM/DD/YYYY)
        Number of Images Bundled:1
              Bundle Name Prefix:spa_4fe2ge
Image #1:
         Name                   :Data & I/O FPGA
         ID                     :1
         Version                :4.17
         Minimal H/W Version    :0.0
         Order in Bundle        :1
         Header Length          :128 bytes
         Data Length            :4951464 bytes
         Total Length           :4951464 bytes (Data + Padding)
         Magic Number           :0xC5C0FDC0
         32-Bit CRC             :0x14613280
         Build Date             :10/12/2004 (MM/DD/YYYY)
```

```
         Image Format          :XSVF
         Upgrade Path          :By Host
         Upgrade Path Info     :0
         Control Flag Value    :0x1
         Estimated Upgrade Time:420 seconds
```

The output in the following example displays information about the FPD image package file stored at a TFTP server location:

```
Router# show upgrade fpd file tftp://mytftpserver/myfpdpkgd/spa-fpd.122-20.S6.pkg
Loading myfpdpkgd/spa-fpd.122-20.S6.pkg from 223.255.254.254 (via FastEthernet0):!
% Extracting compressed bundle spa_4fe2ge-fpd.bndl.zip
...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Content for the "spa_4fe2ge-fpd.bndl" bundle file:
                     Bundle Name:4xFE/2xGE SPA FPD Bundle
                  Bundle Version:0.5
       Number of Supported Cards:2
          Supported Card Type(s):SPA-4FE-7304 (0x435)
                                  SPA-2GE-7304 (0x436)
    Bundle Header Format Version:4
            Bundle Header Length:128 bytes
              Bundle Data Length:4951592 bytes
             Bundle Magic Number:0xC5C0FBC0
               Bundle 32-Bit CRC:0x3B53C5C0
               Bundle Build Date:10/12/2004 (MM/DD/YYYY)
        Number of Images Bundled:1
              Bundle Name Prefix:spa_4fe2ge
Image #1:
         Name                  :Data & I/O FPGA
         ID                    :1
         Version               :4.17
         Minimal H/W Version   :0.0
         Order in Bundle       :1
         Header Length         :128 bytes
         Data Length           :4951464 bytes
         Total Length          :4951464 bytes (Data + Padding)
         Magic Number          :0xC5C0FDC0
         32-Bit CRC            :0x14613280
         Build Date            :10/12/2004 (MM/DD/YYYY)
         Image Format          :XSVF
         Upgrade Path          :By Host
         Upgrade Path Info     :0
         Control Flag Value    :0x1
         Estimated Upgrade Time:420 seconds
[OK - 703488 bytes]
```

Cisco 7600 Series, Catalyst 6500 Series

The output in the following example shows the show upgrade fpd file command on a Cisco 7600 series router and Catalyst 6500 series switch:

```
Router# show upgrade fpd file tftp://mytftpserver/myname/myfpdpkg/c7600-fpd-pkg.122-18.SXE.pkg
Loading myname/myfpdpkg/c7600-fpd-pkg.122-18.SXE.pkg from 124.0.0.0 (via FastEthernet0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK]
Cisco Field Programmable Device Image Package for IOS
C7600 Family FPD Image Package (c7600-fpd-pkg.122-18.SXE.pkg), Version 12.2(SXE)
Copyright (c) 2004-2005 by cisco Systems, Inc.
Built Fri 25-Mar-2005 09:12 by abcdef
=============================== ================================================
```

```
                                       Bundled FPD Image Version Matrix
                                ================================================
                                                                       Min. Req.
Supported Card Types            ID  Image Name                Version  H/W Ver.
=============================== == ========================= ========= =========
2-port T3/E3 Serial SPA          1 T3E3 SPA ROMMON              2.12      0.0
                                 2 T3E3 SPA I/O FPGA            0.24      0.0
                                 3 T3E3 SPA E3 FPGA             0.6       0.0
                                 4 T3E3 SPA T3 FPGA             0.14      0.0
------------------------------- -- ------------------------- --------- ---------
4-port T3/E3 Serial SPA          1 T3E3 SPA ROMMON              2.12      0.0
                                 2 T3E3 SPA I/O FPGA            0.24      0.0
                                 3 T3E3 SPA E3 FPGA             0.6       0.0
                                 4 T3E3 SPA T3 FPGA             0.14      0.0
------------------------------- -- ------------------------- --------- ---------
8-port Channelized T1/E1 SPA     1 CTE1 SPA ROMMON              2.12      0.140
                                 1 CTE1 SPA ROMMON NP           2.12      0.0
                                 2 CTE1 SPA I/O FPGA            1.2       0.0
------------------------------- -- ------------------------- --------- ---------
2-port Channelized T3 SPA        1 CT3 SPA ROMMON               2.12      0.100
                                 2 CT3 SPA I/O FPGA             1.1       0.100
                                 3 CT3 SPA T3 FPGA R1           0.11      0.100
                                 3 CT3 SPA T3 FPGA R2           0.15      0.200
------------------------------- -- ------------------------- --------- ---------
4-port Channelized T3 SPA        1 CT3 SPA ROMMON               2.12      0.100
                                 2 CT3 SPA I/O FPGA             1.1       0.100
                                 3 CT3 SPA T3 FPGA R1           0.11      0.100
                                 3 CT3 SPA T3 FPGA R2           0.15      0.200
------------------------------- -- ------------------------- --------- ---------
2-port OC3 POS SPA               1 POS SPA IOFPGA P1            3.4       0.0
                                 1 POS SPA IOFPGA P2            3.4       0.200
------------------------------- -- ------------------------- --------- ---------
4-port OC3 POS SPA               1 POS SPA IOFPGA P1            3.4       0.0
                                 1 POS SPA IOFPGA P2            3.4       0.200
------------------------------- -- ------------------------- --------- ---------
1-port OC12 POS SPA              1 POS SPA IOFPGA P1            3.4       0.0
                                 1 POS SPA IOFPGA P2            3.4       0.200
------------------------------- -- ------------------------- --------- ---------
2-port OC3 ATM SPA               1 KATM SPA IOFPGA              1.24      0.0
------------------------------- -- ------------------------- --------- ---------
4-port OC3 ATM SPA               1 KATM SPA IOFPGA              1.24      0.0
------------------------------- -- ------------------------- --------- ---------
1-port OC12 ATM SPA              1 KATM SPA IOFPGA              1.24      0.0
------------------------------- -- ------------------------- --------- ---------
SIP-200                          1 SIP-200 I/O FPGA P1          1.1       0.100
                                 1 SIP-200 I/O FPGA P4          1.1       0.400
                                 1 SIP-200 I/O FPGA P6          1.1       0.600
                                 2 SIP-200 EOS FPGA P1          0.27      0.100
                                 2 SIP-200 EOS FPGA P450        1.211     0.450
                                 2 SIP-200 EOS FPGA P5          0.27      0.500
                                 2 SIP-200 EOS FPGA P550        1.211     0.550
                                 2 SIP-200 EOS FPGA P6          1.211     0.600
                                 3 SIP-200 PEG TX FPGA P1       1.129     0.100
                                 3 SIP-200 PEG TX FPGA P6       1.129     0.600
                                 4 SIP-200 PEG RX FPGA P1       1.3       0.100
                                 4 SIP-200 PEG RX FPGA P4       1.3       0.400
                                 4 SIP-200 PEG RX FPGA P6       1.3       0.600
                                 5 SIP-200 ROMMON               1.2       0.100
------------------------------- -- ------------------------- --------- ---------
SIP-400                          1 SIP-400 ROMMON               1.1       0.1
                                 2 SIP-400 I/O FPGA             0.82      0.1
                                 3 SIP-400 SWITCH FPGA          0.25      0.1
------------------------------- -- ------------------------- --------- ---------
CWPA2                            1 CWPA2 I/O FPGA P1            0.37      0.1
```

```
                                 2 CWPA2 EOS FPGA P1            0.28      0.1
                                 3 CWPA2 ROMMON                 1.1       0.1
=============================== ================================================
```

Cisco uBR10012 Universal Broadband Router

The output in the following example displays information about the FPD image package file stored at a TFTP server location:

```
Router# show upgrade fpd file
 tftp://mytftpserver/myname/myfpdpkg/ubr10k-fpd-pkg.122-122_33_SCB_20081123.pkg

Cisco Field Programmable Device Image Package for IOS
UBR10k Family FPD Image Package (ubr10k-fpd-pkg.122-test.pkg), Version 12.2(20080609:181737)
Copyright (c) 2007-2008 by cisco Systems, Inc.
Built Tue 10-Jun-2008 08:42 by dapoirie
=============================== ================================================
                                        Bundled FPD Image Version Matrix
                                ================================================
                                                                    Min. Req.
Supported Card Types            ID  Image Name                Version  H/W Ver.
=============================== == ========================= ========= =========
Modena SPA                       1 MODENA BLAZE FPGA         1285.1444    1.0
------------------------------- -- ------------------------- --------- ---------
5-port GE V2 SPA                 1 GE SPA FPGA                  1.10      0.0
------------------------------- -- ------------------------- --------- ---------
1-port 10GE V2 SPA               1 10GE SPA FPGA                1.9       0.0
=============================== ================================================
```

Related Commands

Command	Description
show hw-module all fpd	Displays the current versions of all FPDs for all of the supported card types on a router.
show hw-module slot fpd	Displays the current versions of all FPDs for a SIP in the specified slot location and for all of the SPAs installed in that SIP or any FPD-capable cards.
show hw-module subslot fpd	Displays the current versions of all FPDs for a particular SPA or all of the active SPAs on a router.
show upgrade fpd package default	Displays which FPD image package is needed for the router to properly support the SPAs or other FPD-capable cards.
show upgrade fpd progress	Displays the progress of the FPD upgrade while an FPD upgrade is taking place.
show upgrade fpd table	Displays various information used by the Cisco IOS software to manage the FPD image package file.
upgrade fpd auto	Configures the router to automatically upgrade the FPD image when an FPD version incompatibility is detected.
upgrade fpd path	Specifies the location from where the FPD image package should be loaded when an automatic FPD upgrade is initiated by the router.

Command	Description
upgrade hw-module slot	Manually upgrades the current FPD image package on a SIP or any FPD-capable cards.
upgrade hw-module subslot	Manually upgrades the current FPD image on the specified SPA.

show upgrade fpd package default

To display which FPD image package is needed for the router to properly support the SPAs or other FPD-capable cards for the running Cisco IOS release, enter the **showupgradefpdpackagedefault** command in privileged EXEC mode.

show upgrade fpd package default

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(20)S6	This command was introduced and replaced the **showupgradepackagedefault**command on the Cisco 7304 router.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(4)XD	This command was integrated into Cisco IOS Release 12.4(4)XD.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.

Usage Guidelines

It is important to note that the output from this command is generated from the Cisco IOS image and provides information regarding the default FPD image package file that is needed for your particular Cisco IOS release. This command output also lists the SPAs or other cards supported by the default FPD image package file for the running Cisco IOS image.

In Cisco IOS Releases 12.2(20)S2 through 12.2(20)S5, the output generated by entering this command can be generated by entering the **showupgradepackagedefault**command.

For more information about FPD upgrades on SPA interface processors (SIPs) and shared port adapters (SPAs), see the Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide.

Examples

Cisco 7200 VXR

The following example shows which cards are supported with your current Cisco IOS release and which FPD image package you need:

```
Router# show upgrade fpd package default
```

```
***********************************************************************
This IOS release requires the following default FPD Image Package for
the automatic upgrade of FPD images:
***********************************************************************
Version: 12.4(4)XD
Package Filename: c7200-fpd-pkg.124-4.XD.pkg
        List of card type supported in this package:
                                        Minimal
                 No. Card Type          HW Ver.
                ---- ------------------ -------
                  1) VSA                  0.0
                  2) NPE-G2               0.0
                ---- ------------------ -------
***********************************************************************
```

Cisco 7304

In the following example, the **showupgradefpdpackagedefault** command output shows that the spa_fpd.122-20-S6.pkg FPD image package file is required if you install the SPA-4FE-7304 or the SPA-2GE-7304 on this particular router with this particular Cisco IOS software release:

```
Router# show upgrade fpd package default
***********************************************************************
This IOS release supports the following default FPD Image Package(s) for
automatic upgrade:
***********************************************************************
SPA FPD Image Package:spa_fpd.122-20.S6.pkg
        List of SPAs supported in this package:
                                        Minimal
                 No. SPA Name           HW Ver.
                ---- ------------------ -------
                  1) SPA-4FE-7304         0.0
                  2) SPA-2GE-7304         0.0
                ---- ------------------ -------
```

Cisco uBR10012 Universal Broadband Router

In the following example, the **showupgradefpdpackagedefault** command output shows that the ubr10k-fpd-pkg.122-122_33_SCB_20081123.pkg FPD image package file is required for the SPAs on this particular router with this particular Cisco IOS software release:

```
Router# show upgrade fpd package default
****************************************************************************
This Cisco IOS software image requires the following default FPD Image
Package for the automatic upgrade of FPD images (the package is available
from Cisco.com and is accessible from the Cisco Software Center page where
this IOS software image can be downloaded):
****************************************************************************

Version: 12.2(20080919:205903)

Package Filename: ubr10k-fpd-pkg.122-122_33_SCB_20081123.pkg

        List of card type supported in this package:

                                                              Minimal
                 No. Card Type                                HW Ver.
                ---- ---------------------------------------- -------
```

```
  1) 5xGE SPA                                   0.0
  2) 1x10GE XFP SPA                             0.0
  4) WIDEBAND DOCSIS SPA                        0.0
---- ---------------------------------------- -------
```

Related Commands

Command	Description
show hw-module all fpd	Displays the current versions of all FPDs for all of the supported card types on a router.
show hw-module slot fpd	Displays the current versions of all FPDs for a SIP in the specified slot location and for all of the SPAs installed in that SIP or any FPD-capable cards.
show hw-module subslot fpd	Displays the current versions of all FPDs for a particular SPA or all of the active SPAs on a router.
show upgrade fpd file	Displays the contents of an FPD image package file.
show upgrade fpd progress	Displays the progress of the FPD upgrade while an FPD upgrade is taking place.
show upgrade fpd table	Displays various information used by the Cisco IOS software to manage the FPD image package file.
upgrade fpd auto	Configures the router to automatically upgrade the FPD image when an FPD version incompatibility is detected.
upgrade fpd path	Specifies the location from where the FPD image package should be loaded when an automatic FPD upgrade is initiated by the router.
upgrade hw-module slot	Manually upgrades the current FPD image package on a SIP or any FPD-capable cards.
upgrade hw-module subslot	Manually upgrades the current FPD image on the specified SPA.

show upgrade fpd progress

To view the progress of an FPD upgrade while an FPD upgrade is taking place, enter the **showupgradefpdprogress** command in privileged EXEC mode.

show upgrade fpd progress

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(20)S6	This command was introduced and replaced the **showupgradeprogress** command on the Cisco 7304 router.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(4)XD	This command was integrated into Cisco IOS Release 12.4(4)XD.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.

Usage Guidelines

In Cisco IOS Releases 12.2(20)S2 through 12.2(20)S5, the output generated by entering this command can be generated by entering the **showupgradeprogress**command.

For more information about FPD upgrades on SPA interface processors (SIPs) and shared port adapters (SPAs), refer to the Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide.

Examples

Cisco 7200 VXR

The following example shows that the FPD image is being updated, the approximate amount of time needed to perform the update, and the amount of time the FPD update has taken so far:

```
Router# show upgrade fpd progress
FPD Image Upgrade Progress Table:
 ==== =================== ====================================================
                                                     Approx.
                          Field Programmable   Time      Elapsed
 Slot Card Type           Device : "ID-Name"   Needed      Time    State
 ==== =================== ================== ========== ========== ===========
```

```
  npe NPE-G2 IOFPGA       1-NPEG2 I/O FPGA    00:01:00   00:00:23  Updating...
 ==== =================== ====================================================
```

Cisco 7304

The following example shows the status of FPD updates on the SPAs located in subslots 0 and 1:

```
Router# show upgrade fpd progress
FPD Image Upgrade Progress Table:
 ==== =================== ====================================================
                          Field Programmable    Time
 Slot Card Description    Device :"ID-Name"    Needed   Time Left  State
 ==== =================== ================== ========== ========== ===========
  2/0 SPA-2GE-7304        1-4FE/2GE FPGA      00:06:00   00:05:17  Updating...
 ---- ------------------- ------------------ ----------- --------- -----------
  2/1 SPA-4FE-7304        1-4FE/2GE FPGA      --:--:--   --:--:--  Waiting...
 ==== =================== ====================================================
```

Cisco uBR10012 Universal Broadband Router

The following example shows the status of FPD updates on a Cisco uBR10012 router:

```
Router# show upgrade fpd progress
FPD Image Upgrade Progress Table:
==== =================== ====================================================
                                               Approx.
                          Field Programmable    Time     Elapsed
 Slot Card Type           Device : "ID-Name"   Needed      Time    State
 ==== =================== ================== ========== ========== ===========
  3/2 SPA-24XDS-SFP       1-Modena BLAZE FPG  00:10:00   00:05:07  Updating...
 ==== =================== ====================================================
```

Related Commands

Command	Description
show hw-module all fpd	Displays the current versions of all FPDs for all of the supported card types on a router.
show hw-module slot fpd	Displays the current versions of all FPDs for a SIP in the specified slot location and for all of the SPAs installed in that SIP or any FPD-capable cards.
show hw-module subslot fpd	Displays the current versions of all FPDs for a particular SPA or all of the active SPAs on a router.
show upgrade fpd file	Displays the contents of an FPD image package file.
show upgrade fpd package default	Displays which FPD image package is needed for the router to properly support the SPAs or other FPD-capable cards.
show upgrade fpd table	Displays various information used by the Cisco IOS software to manage the FPD image package file.
upgrade fpd auto	Configures the router to automatically upgrade the FPD image when an FPD version incompatibility is detected.

Command	Description
upgrade fpd path	Specifies the location from where the FPD image package should be loaded when an automatic FPD upgrade is initiated by the router.
upgrade hw-module slot	Manually upgrades the current FPD image package on a SIP or any FPD-capable cards.
upgrade hw-module subslot	Manually upgrades the current FPD image on the specified SPA.

show upgrade fpd table

To view various information used by the Cisco IOS software to manage the FPD image package file, use the **showupgradefpdtable** command in privileged EXEC mode.

show upgrade fpd table

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(20)S6	This command was introduced and replaced the **showupgradetable**command on the Cisco 7304 router.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.

Usage Guidelines

This command provides version information used by the Cisco IOS image to manage the FPD image package file and to locate the correct FPD image within the FPD image package file to perform an FPD upgrade. Most of the information provided by this command is useful for customer support purposes.

In Cisco IOS Releases 12.2(20)S2 through 12.2(20)S5, the output generated by entering this command can be generated by entering the **showupgradetable**command.

For more information about FPD upgrades on SPA interface processors (SIPs) and shared port adapters (SPAs), refer to the Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide.

Examples

The following example displays various FPD information for Cisco IOS Release 12.2(20)S5:

```
Router# show upgrade fpd table

Field Programmable Devices (FPD) Bundle Information Table:
==========================================================

Table Entry #1:

       Bundle Card Type:SPA-4FE-7304 (0x435)
        Platform Family:0x0
     Bundle Name Prefix:spa_4fe2ge
         Bundle Version:0.5
    Minimal H/W Version:0.0
        FPD Image Count:1
     FPD Image Required:
                                                        Min. Required
```

```
                         FPD ID FPD Name                 Version
                         ------ ------------------------ -------------
                            1   Data & I/O FPGA           4.17
                         ------ ------------------------ -------------

Table Entry #2:

       Bundle Card Type:SPA-2GE-7304 (0x436)
        Platform Family:0x0
     Bundle Name Prefix:spa_4fe2ge
         Bundle Version:0.5
    Minimal H/W Version:0.0
        FPD Image Count:1
     FPD Image Required:
                                                         Min. Required
                         FPD ID FPD Name                 Version
                         ------ ------------------------ -------------
                            1   Data & I/O FPGA           4.17
                         ------ ------------------------ -------------
```

Cisco uBR10012 Universal Broadband Router

The following example displays various FPD information for Cisco IOS Release 12.2(33)SCB:

```
Router# show upgrade fpd table
```

Field Programmable Devices (FPD) Bundle Information Table:

```
==========================================================
Table Entry #1:
       Bundle Card Type: 5xGE SPA (0x50A)
            Card Family: SPA
        Platform Family: 0x0
     Bundle Name Prefix: spa_ge_eth
         Bundle Version: 0.1
    Minimal H/W Version: 0.0
        FPD Image Count: 1
     FPD Image Required:
                                                         Min. Required
                         FPD ID FPD Name                 Version
                         ------ ------------------------ -------------
                            1   5xGE V2 I/O FPGA          1.10
                         ------ ------------------------ -------------

Table Entry #2:

       Bundle Card Type: 1x10GE XFP SPA (0x50C)
            Card Family: SPA
        Platform Family: 0x0
     Bundle Name Prefix: spa_10ge_eth
         Bundle Version: 0.1
    Minimal H/W Version: 0.0
        FPD Image Count: 1
     FPD Image Required:
                                                         Min. Required
                         FPD ID FPD Name                 Version
                         ------ ------------------------ -------------
                            1   10GE V2 I/O FPGA          1.9
                         ------ ------------------------ -------------
Table Entry #3:
```

```
Bundle Card Type: WIDEBAND DOCSIS SPA (0x4AE)
            Card Family: SPA
        Platform Family: 0x0
     Bundle Name Prefix: spa_modena
         Bundle Version: 0.5
    Minimal H/W Version: 0.0
        FPD Image Count: 1
     FPD Image Required:
                                                            Min. Required
                         FPD ID FPD Name                        Version
                         ------ ------------------------ -------------
                            1   Modena BLAZE FPGA          1285.1444
                         ------ ------------------------ -------------
```

Related Commands

Command	Description
upgrade hw-module subslot	Manually upgrades the current FPD image on the specified SPA.
upgrade fpd auto	Configures the router to automatically upgrade the FPD image when an FPD version incompatability is detected.
upgrade fpd path	Specifies the location from where the FPD image package should be loaded when an automatic FPD upgrade is initiated by the router.
show hw-module slot fpd	Displays the current versions of FPD image files for all of the active SIPs on a router.
show hw-module subslot fpd	Displays the FPD version on each SPA in the router.
show upgrade fpd file	Displays the contents of an FPD image package file.
show upgrade fpd package default	Displays which FPD image package is needed for the router to properly support the SPAs.
show upgrade fpd progress	Displays the progress of the FPD upgrade while an FPD upgrade is taking place.

show upgrade fpga progress

To display the progress of an FPGA upgrade on a Cisco 7304 router, use the **showupgradefpgaprogress**command in privileged EXEC mode.

show upgrade fpga progress

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(20)S6	This command was introduced.

Usage Guidelines

This command will only provide useful output during an FPGA upgrade.

This command provides information regarding FPGA upgrades, including the approximate amount of time a particular FPGA upgrade would take and the amount of time the in-progress FPGA upgrade has taken.

Because the console where you began the FPGA upgrade becomes unusable during the FPGA upgrade, this command can only be entered from a connection that was not used to initiate the FPGA upgrade.

Examples

The following example displays information about an in-progress FPGA update. Note that the example shows the FPGA mismatch and provides the user with the approximate time needed to complete the upgrade and the amount of time the current upgrade has taken.

```
Router# show upgrade fpga progress
FPGA image update progress information:
  Slot 0, FPGA name = NPEG100
  Hardware version = 01.00
  Current FPGA version = 02.04
  New FPGA version = 02.05
  Time needed to update = 00:12:00 (approximate)
  Actual time taken so far = 00:01:47
```

Related Commands

Command	Description
show c7300	Displays the types of hardware installed in a Cisco 7304 router, including the current FPGA version and the bundled FPGA version.
show diag	Displays hardware information for any slot or the chassis.
upgrade fpga	Specifies router response when an FPGA mismatch is detected.
upgrade fpga all	Manually upgrades all of the FPGAs for all of the installed hardware on the Cisco 7304 router.

show upgrade hw-programmable file

To display the names and versions of individual files in the hw-programmable package file in a Cisco ASR 1000 Series Router, use the **showupgradehw-programmablefile**command in Privileged EXEC configuration mode.

show upgrade hw-programmable file filename

Syntax Description

filename	Specifies the hw-programmable upgrade package file and its file system location. For filename, specify one of the following system locations and a package file name: • bootflash: RP-relative HW programmable package name • flash: RP-relative HW programmable package name • harddisk: RP-relative HW programmable package name This is the hw-programmable upgrade package file that contains a new version of the CPLD and FPGA code, used for performing the CPLD on a Cisco ASR 1013 Router or FPGA upgade on a Cisco ASR 1000 Series Router. The package file name is typically named asr1000-hw-programmables.<release_name>.pkg

Command Default

The names and versions of individual files in the hw-programmable package file is not displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced in Cisco IOS XE Release 3.1S.

Usage Guidelines

For procedures on performing a CPLD upgrade, see the Upgrading Field Programmable Hardware Devices for Cisco ASR 1000 Series Routers document.

Examples

The following example displays the names of the card types and version numbers in the package file:

```
Router# show upgrade hw-programmable file harddisk:asr1000-hw-programmables.xe31.100616.pkg

  List of card type, hw-programmable device and version in this package:
  No.  Card Type           hw-programmable device  Version
--------------------------------------------------------------
   0   ASR1000-SIP10       CPLD                    09111601
   1   ASR1000-RP2         CPLD                    10021901
```

Related Commands

Command	Description
upgrade hw-programmable	Performs a Complex Programmable Logic Device (CPLD) or Field-Programmable Gate Array (FPGA) upgrade on a Cisco ASR 1000 Series Router.
show hw-programmable	Displays the current CPLD and FPGA versions on a Cisco ASR 1000 Series Router.
show upgrade hw-programmable progress	Displays the upgrade progress of the line card-field upgradeable device (LC-FPD) on a Cisco ASR 1000 Series Router.

show upgrade hw-programmable progress

To display the upgrade progress of the line card-field upgradeable device (LC-FPD) on a Cisco ASR 1000 Series Router, use the **showupgradehw-programmableprogress**command in Privileged EXEC configuration mode.

show upgrade hw-programmable progress

Syntax Description

This command has no arguments or keywords.

Command Default

The upgrade progress of the line card-field upgradeable device is not displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced in Cisco IOS XE Release 3.1S.

Usage Guidelines

The line card may be an RP, ESP, or SIP card.

This command only displays the hardware programmable upgrades that are in progress.

For procedures on performing a CPLD upgrade, see the Upgrading Field Programmable Hardware Devices for Cisco ASR 1000 Series Routers document.

Examples

The following example displays the upgrade progress of the CPLD upgrade in the RP slot 1:

```
Router# show upgrade hw-programmable progress

Upgrade hw-programmable progress

Slot              Hw-programmable device    Upgrade status
------------------------------------------------------------
R1                CPLD                      in progress
```

Related Commands

Command	Description
upgrade hw-programmable	Performs a Complex Programmable Logic Device (CPLD) or Field-Programmable Gate Array (FPGA) upgrade on a Cisco ASR 1000 Series Router.
show hw-programmable	Displays the current CPLD and FPGA version on a Cisco ASR 1000 Series Router.
show upgrade hw-programmable	Displays the names and versions of individual files in the hw_programmable package file.

show upgrade package default

The show upgrade package default command is replaced by the **show upgrade fpd package default** command. See the **show upgrade fpd package default** command for more information.

show upgrade progress

The show upgrade progress command is replaced by the **show upgrade fpd progress** command. See the **show upgrade fpd progress** command for more information.

show upgrade table

The show upgrade table command is replaced by the **show upgrade fpd table** command. See the **show upgrade fpd table** command for more information.

show vmi neighbors

To display information about neighbor connections to the Virtual Multipoint Interface (VMI), use the **showvmineighbors** command in User EXEC mode.

show vmi neighbors [**detail**] [*vmi-interface*]

Syntax Description

detail	(Optional) Displays details about the VMI neighbors.
vmi-interface	(Optional) Number of the VMI interface

Command Default

If no arguments are specified, information about all neighbors for all VMI interfaces is displayed.

Command Modes

User EXEC

Command History

Release	Modification
12.4(15)XF	This command was introduced.
12.3(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

If no arguments are specified, information about all neighbors for all VMI interfaces is displayed.

The **showvmineighbors**command provides a list of devices that have been dynamically discovered by the connected radio devices in a router-to-radio network, and for which connectivity has been achieved through PPPoE and the radio network.

Examples

The following is sample output from the **showvmineighbors** command used to display dynamically created neighbors on a VMI interface.

```
Router# show vmi neighbors vmi1
1 vmi1 Neighbors
           IPV6       IPV4                          Transmit    Receive
Interface  Address    Address        Uptime       Packets     Packets
vmi1       ::         10.3.3.2       00:02:11     0000000008  0000000073
```

The table below describes the significant fields shown in the **showvmineighbors** command display.

Table 275: show vmi neighbors Field Descriptions

Field	Description
Interface	The interface number.
IPv6 Address	IPv6 address of the neighbor.
IPv4 Address	IPv4 address of the neighbor.
Uptime	How long the interface has been up. Time shown in hh:mm:ss format.
Transmit Packets	Number of packets transmitted from the interface during the monitored up time.

Field	Description
Received Packets	Number of packets received on the interface during the monitored up time.

show vmi neighbors command with detail keyword: Example

The following example shows the details about the known VMI neighbors.

```
Router# show vmi neighbors detail

1 vmi1 Neighbors
vmi1   IPV6 Address=::
       IPV4 Address=10.3.3.2, Uptime=00:02:16
       Output pkts=8, Input pkts=75
       No Session Metrics have been received for this neighbor.
       Transport PPPoE, Session ID=79
       INTERFACE STATS:
          VMI Interface=vmi1,
             Input qcount=0, drops=0, Output qcount=0, drops=0
          V-Access intf=Virtual-Access3,
             Input qcount=0, drops=0, Output qcount=0, drops=0
          Physical intf=FastEthernet0/0,
             Input qcount=0, drops=0, Output qcount=0, drops=0
PPPoE Flow Control Stats
 Local Credits: 65442   Peer Credits: 65443
 Credit Grant Threshold: 28000    Max Credits per grant: 65534
 PADG Seq Num: 133     PADG Timer index: 0
 PADG last rcvd Seq Num: 133
 PADG last nonzero Seq Num: 0
 PADG last nonzero rcvd amount: 0
 PADG Timers:    [0]-1000    [1]-2000    [2]-3000    [3]-4000
 PADG xmit: 133  rcvd: 133
 PADC xmit: 133  rcvd: 133
 PADQ xmit: 0  rcvd: 0
```

The table below describes the significant fields shown in the **showvmineighborsdetail**command display.

Table 276: show vmi neighbors detail Field Descriptions

Field	Description
Interface	The interface number.
IPv6 Address	IPv6 address of the neighbor.
IPv4 Address	IPv4 address of the neighbor.
Uptime	How long the interface has been up. Time shown in hh:mm:ss format.
Output pkts	Number of outgoing packets during the recorded up time.
Input pkts	Number of incoming packets during the recorded up time.
Transmitted packets	Number of packets transmitted from the interface.
Received Packets	Number of packets received on the interface.

Field	Description
Transport	The routing protocol, in this case-PPPoE.
Session ID	The identifier of the VMI session.
INTERFACE STATS	A series of statistics collected on the interface and shows for each of the VMI interface, virtual access interface, and the physical interface. For each interface, statistics are displayed indicating the number of packets in the input and output queues and the number of packets dropped from each queue.
PPPoE Flow Control Stats	The statistics collected for PPPoE credit flow. **Local Credits** : The amount of credits belonging to this node.**PeerCredits**: The amount of credits belonging to the peer.**CreditGrantThreshold**: The number of credits below which the peer needs to dip before this node sends an inband or out-of-band grant.**MaxCreditspergrant**: 65534**PADGSeqNum**: 133 **PADGTimerindex**: 0**PADGlastrcvdSeqNum**: 133**PADGlastnonzeroSeqNum**: 0**PADGlastnonzerorcvdamount**: 0**PADGTimers**: [0]-1000 [1]-2000 [2]-3000 [3]-4000**PADGxmit**:*numberic***rcvd**: *numeric* **PADCxmit**:**133rcvd:133** **PADQxmit**:**0rcvd**: 0

Related Commands

Command	Description
debug vmi	Displays debugging output for virtual multipoint interfaces (VMIs)
interface vmi	Creates a virtual multipoint interface (VMI) that can be configured and applied dynamically.

show wedged-interfaces

To display input and output queue wedged interfaces, use the **showwedged-interfaces** command in user EXEC or privileged EXEC mode.

show wedged-interfaces {**input** | **output**}

Syntax Description

input	Displays input the queue wedged interface list.
output	Displays output the queue wedged interface list.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M on the Cisco AS 5400 series routers.

Usage Guidelines

Interface queue wedged monitoring is disabled by default. You can use the **interface-monitorenable** command to enable the queue wedged monitoring. Once the monitoring is switched on, a background process is created, which monitors all the existing input and output queue wedged interfaces.

Examples

The following is sample output from the **showwedged-interfaces** command:

```
Router# show wedged-interfaces output
Interface Name             Time Since Wedge
Async4/00                  00:23:33
Async4/01                  00:23:26
Async4/02                  00:23:21
Async4/03                  00:23:15
FastEthernet0/0            00:24:35
FastEthernet0/1            00:24:50
Virtual-Access2            00:38:19
Virtual-Access3            00:38:19
```

The table below describes the fields shown in the display.

Table 277: show wedged-interfaces output Field Descriptions

Field	Description
Interface Name	Lists the name of the interface.
Time Since Wedge	Time since a problem was detected in the interface.

Related Commands

Command	Description
interface-monitor enable	Enables interface queue wedge monitoring.

shutdown (controller)

To disable the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 or Cisco 10000 series routers, use the **shutdown**command in controller configuration mode. To restart a disabled CT3IP, use the **no** form of this command.

shutdown
no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

Using this command assumes that the controller is already enabled. By default, if this command is not issued, the controller remains enabled.

Command Modes

Controller configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Cisco 7500 Series Routers

Shutting down the CT3IP disables all functions on the interface and sends a blue alarm to the network. The **shutdown** command marks the interface as unavailable. To check if the CT3IP is disabled, use the **showcontrollerst3** command.

Cisco 10000 Series Router

Alarms are cleared automatically 10 seconds after a no shutdown command is issued on a T3 port. Shutting down a controller causes a T3 port to transmit:

- A blue alarm for m13 framing
- An idle signal for c-bit framing

There is no delay for alarms to clear after issuing a no shutdown command on an E3 port.

Examples

Cisco 7500 Series Router

The following example shuts down the CT3IP:

```
Router(config
)
# controller t3 9/0/0
```

```
Router(config
-controller)
# shutdown
```

Cisco 10000 Series Router

The following example shuts down the controller on port 0:

```
Router(config
)
# dsx3 1/0/0
Router(config
-controller)
# shutdown
```

Related Commands

Command	Description
show controllers j1	Displays information about the J1 link.
show controllers t1	Displays the total number of calls and call durations on a T1 controller.
show controllers t3	Displays the hardware and software driver information for a T3 controller.

shutdown (dwdm)

To disable DWDM controller processing, use the **shutdown** command in controller configuration mode. To bring a DWDM controller back up and enable DWDM controller processing, use the**no** form of this command.

shutdown
no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
12.2(33)SRD1	This command was introduced on the Cisco 7600 series router.

Usage Guidelines

The DWDM controller is enabled by default. You must use the shutdown command to disable the controller.

Examples

The following example disables the DWDM controller :

```
Router(config)# controller dwdm 1/1
Router(config-controller)# shutdown
```

Related Commands

Command	Description
show controller dwdm	Displays ITU-T G.709 alarms, alerts, and counters.

shutdown (hub)

To shut down a port on an Ethernet hub of a Cisco 2505 or Cisco 2507 router, use the **shutdown**command in hub configuration mode. To restart the disabled hub, use the **no** form of this command.

shutdown
no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

Using this command assumes that the hub is already enabled. By default, if this command is not issued, the hub remains enabled.

Command Modes

Hub configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shuts down hub 0, ports 1 through 3:

```
Router(config)#
 hub ethernet 0 1 3
Router(config-hub)#
 shutdown
```

Related Commands

Command	Description
hub	Enables and configures a port on an Ethernet hub of a Cisco 2505 or Cisco 2507 router.

shutdown (interface)

To disable an interface, use the **shutdown** command in interface configuration mode. To restart a disabled interface, use the **no**form of this command.

shutdown
no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

Using this command assumes that the interface is already enabled. By default, if this command is not issued, the interface remains enabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **shutdown** command disables all functions on the specified interface. On serial interfaces, this command causes the data terminal ready (DTR) signal to be dropped. On Token Ring interfaces, this command causes the interface to be removed from the ring. On FDDI interfaces, this command causes the optical bypass switch, if present, to go into bypass mode.

This command also marks the interface as unavailable. To check whether an interface is disabled, use the **showinterfaces** user EXEC command; an interface that has been shut down is shown as administratively down in the display from this command.

Examples

The following example turns off Ethernet interface 0:

```
Router(config
)
# interface ethernet 0
Router(config-if
)
# shutdown
08:32:03:%LINK-5-CHANGED:Interface Ethernet 0, changed state to administratively down
```

The following example turns the interface back on:

```
Router(config
)
# interface ethernet 0
Router(config
-if)
```

```
# no shutdown
08:32:16:%LINK-3-UPDOWN:Interface Ethernet 0, changed state to up
08:32:17:%LINEPROTO-5-UPDOWN:Line protocol on Interface Ethernet 0, changed state to up
```

Related Commands

Command	Description
interface	Configures an interface type and enters interface configuration mode.
show interfaces	Displays the statistical information specific to a serial interface.

signaling

To enable channel-associated signaling (CAS), use the **signaling**command in CEM configuration mode. To disable signaling, use the **no** form of this command.

signaling [*on-hook-pattern*] [*off-hook-pattern*] [*msec*]
no signaling [*on-hook-pattern*] [*off-hook-pattern*] [*msec*]

Syntax Description

on-hook-pattern	(Optional) Specifies the ABCD signaling bits sent to the attached device (typically a PBX) to simulate the remote PBX sending notification that any call in progress has been terminated or is on-hook. The T1 default is 5 hex. The E1 default is D hex.
off-hook-pattern	(Optional) Specifies the ABCD signaling bits sent to the attached device (typically a PBX) to simulate the remote PBX sending notification that a channel is already in use, or is off-hook. The T1 default is F hex. The E1 default is 5 hex.
msec	(Optional) Specifies the time, in milliseconds, between the onhook and offhook patterns. Values are in the range from 50 to 5000. Default is 2000. Any value entered is rounded up to the next multiple of 50 milliseconds.

Command Default

CAS is disabled.

Command Modes

CEM configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.3(7)T1	The *on-hook-pattern*, *off-hook-pattern*, and *msec* arguments were added.

Usage Guidelines

When a T1/E1 channel with signaling enabled is placed in the failed state, the on-hook pattern is sent to the attached device for a duration specified by the *msec* attribute. After the time specified by the *msec*attribute, the off-hook pattern is sent to the attached device for as long as the CEM connection remains failed.

The on-hook pattern parameter specifies, as a single hexadecimal character, the ABCD signaling bits sent to the attached device (typically a PBX) to simulate the remote PBX sending notification that any call in progress has been terminated or is on-hook. This provides a forced disconnect of any calls when the CEM connection fails.

The off-hook pattern parameter specifies, as a single hexadecimal character, the ABCD signaling bits sent to the attached device (typically a PBX) to simulate the remote PBX sending notification that a channel is already in use, or is off-hook. This prevents the attached PBX from trying to use the failed channel to place a new call while the CEM connection remains failed.

Examples

The following example shows how to enable signaling.

```
Router(config-cem)# signaling
```

The following example shows how to enable signaling with onhook and offhook parameters:

```
Router(config-cem)# signalling 0x0 0x1 101
Delay will be set to 150 ms
```

Related Commands

Command	Description
cem	Enters circuit emulation configuration mode.
failure	Specifies a time period before a CEM connection enters, or recovers from, a failed state.
show cem	Displays CEM channel statistics.

smt-queue-threshold

To set the maximum number of unprocessed FDDI station management (SMT) frames that will be held for processing, use the **smt-queue-threshold** command in global configuration mode. To restore the queue to the default, use the **no** form of this command.

smt-queue-threshold *number*
no smt-queue-threshold

Syntax Description

number	Number of buffers used to store unprocessed SMT messages that are to be queued for processing. Acceptable values are positive integers. The default value is equal to the number of FDDI interfaces installed in the router.

Command Default

The default threshold value is equal to the number of FDDI interfaces installed in the router.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command helps ensure that routers keep track of FDDI *upstream* and *downstream* neighbors, particularly when a router includes more than one FDDI interface.

In FDDI, upstream and downstream neighbors are determined by transmitting and receiving SMT Neighbor Information Frames (NIFs). The router can appear to lose track of neighbors when it receives an SMT frame and the queue currently contains an unprocessed frame. This occurs because the router discards incoming SMT frames if the queue is full. Discarding SMT NIF frames can cause the router to lose its upstream or downstream neighbor.

Caution Use this command carefully because the SMT buffer is charged to the inbound interface (input hold queue) until the frame is completely processed by the system. Setting this value to a high limit can impact buffer usage and the ability of the router to receive routable packets or routing updates.

Examples

The following example specifies that the SMT queue can hold ten messages. As SMT frames are processed by the system, the queue is decreased by one:

```
Router(config)# smt-queue-threshold 10
```

snmp ifmib ifindex persist

To globally enable ifIndex values to persist , which will remain constant across reboots, for use by the Simple Network Management Protocol (SNMP), use the **snmpifmibifindexpersist**command in global configuration mode. To globally disable ifIndex persistence, use the **no** form of this command.

snmp ifmib ifindex persist
no snmp ifmib ifindex persist

Syntax Description

This command has no arguments or keywords.

Command Default

The ifIndex persistence on a router is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRA	This command was introduced. This command replaces the **snmp-serverifindexpersist**command.
12.2(31)SG	This command was integrated into Cisco IOS Release 12.2(31)SG.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **snmpifmibifindexpersist** command does not override an interface-specific configuration. The interface-specific configuration of ifIndex persistence is configured with the **snmpifindexpersist** and **snmpifindexclear** commands in interface configuration mode.

The **snmpifmibifindexpersist** command enables ifIndex persistence for all interfaces on a routing device by using the ifDescr and ifIndex entries in the ifIndex table of interface MIB (IF-MIB).

ifIndex persistence means that the ifIndex values in the IF-MIB persist across reboots, allowing for the consistent identification of specific interfaces that use SNMP.

If ifIndex persistence was previously disabled for a specific interface by using the **nosnmpifindexpersist** command, ifIndex persistence will remain disabled for that interface.

Examples

The following example shows how to enable ifIndex persistence for all interfaces:

```
Router(config)# snmp ifmib ifindex persist
```

Related Commands

Command	Description
snmp ifindex clear	Clears any previously configured **snmpifIndex** commands issued in interface configuration mode for a specific interface.
snmp ifindex persist	Enables ifIndex values that persist across reboots (ifIndex persistence) in the IF-MIB.

snmp ifindex clear

To clear previously configured Simple Network Management Protocol (SNMP) ifIndex commands issued for a specific interface or a specific service instance, use the **snmpifindexclear** command in either interface configuration mode or service instance configuration mode. This command does not have a **no** form.

snmp ifindex clear

Syntax Description

This command has no arguments or keywords.

Command Default

ifIndex values are not cleared.

Command Modes

Interface configuration (config-if) Service instance configuration (config-if-srv)

Command History

Release	Modification
12.0(11)S	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRD1	Support for this command was extended to service instance configuration mode in Cisco IOS Release 12.2(33)SRD1.

Usage Guidelines

Interface Index Persistence means that ifIndex values in the IF-MIB persist across reboots, allowing for consistent identification of specific interfaces using SNMP.

Use the**snmpifindexclear** command on a specific interface when you want that interface to use the global configuration setting for ifIndex persistence. This command clears all ifIndex configuration commands previously entered for that specific interface.

When you clear the ifIndex configuration, the ifIndex persistence is enabled for all interfaces as specified by the **snmp-serverifindexpersist** command in global configuration mode.

Examples

The following example shows how to enable ifIndex persistence for all interfaces:

```
Router(config)# snmp-server ifindex persist
```

The following example shows how to disable IfIndex persistence for Ethernet interface 0/1:

```
Router(config)# interface ethernet 0/1
Router(config-if)# no snmp ifindex persist
Router(config-if)# exit
```

The following example shows how to clear ifIndex persistence for service instance 100 on Ethernet interface 0/1:

```
Router(config)# interface ethernet 0/1
Router(config-if)# service instance 100 ethernet

Router(config-if-srv)# snmp ifindex clear
```

Router(config-if-srv)# **exit**

The following example shows how to clear the ifIndex configuration from Ethernet interface 0/1:

```
Router(config)# interface ethernet 0/1
Router(config-if)# snmp ifindex clear
Router(config-if)# exit
```

The ifIndex persistence configuration is now enabled for all interfaces, as specified by the **snmp-serverifindexpersist** global configuration command.

Related Commands

Command	Description
snmp ifindex persist	Enables ifIndex values in the Interfaces MIB (IF-MIB) that persist across reboots (ifIndex persistence) only on a specific interface.
snmp-server ifindex persist	Enables ifIndex values that will remain constant across reboots for use by SNMP.

snmp-server enable traps netsync

To configure the Simple Network Management Protocol (SNMP) SyncE trap, use the**snmp-serverenabletrapsnetsync**command in global configuration mode. To disable the SNMP SyncE trap, use the **no** form of this command.

snmp-server enable traps netsync
no snmp-server enable traps netsync

Syntax Description

This command has no arguments or keywords.

Command Default

SNMP traps are not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(2)S	This command was introduced.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

The **showrunning-config**command when used with the **trap** keyword displays the SNMP traps that are enabled on a device.

Examples

The following example shows how to enable the SNMP traps on the SyncE event:

```
Device# configure terminal
Device(config)# snmp-server enable traps netsync
Device(config)# end
```

Related Commands

Command	Description
show running-config	Displays the running configuration of the device.

snmp ifindex persist

To enable ifIndex values in the Interfaces MIB (IF-MIB) that persist across reboots (ifIndex persistence) on a specific interface or service instance, use the **snmpifindexpersist**command in either interface configuration mode or service instance configuration mode. To disable ifIndex persistence on a specific interface or service instance, use the **no** form of this command.

snmp ifindex persist
no snmp ifindex persist

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled.

Command Modes

Interface configuration (config-if) Service instance configuration (config-if-srv)

Command History

Release	Modification
12.0(11)S	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRD1	Support for this command was extended to service instance configuration mode in Cisco IOS Release 12.2(33)SRD1.

Usage Guidelines

Interface Index Persistence means that ifIndex values in the IF-MIB persist across reboots, allowing for consistent identification of specific interfaces using Simple Network Management Protocol (SNMP).

The **snmpifindexpersist** command in interface configuration mode enables and disables ifIndex persistence for individual entries (corresponding to individual interfaces) in the ifIndex table of the IF-MIB.

The **snmpifindexpersist** command in service instance configuration mode enables and disables ifIndex persistence for individual service instances (Layer 2 VLAN interfaces) in the ifIndex table of the IF-MIB.

The **snmp-serverifindexpersist** command in global configuration mode enables and disables ifIndex persistence for all interfaces on the routing device that have ifDescr and ifIndex entries in the ifIndex table of the IF-MIB.

IfIndex commands configured for an interface apply to all subinterfaces on that interface.

Examples

In the following example, ifIndex persistence is enabled for Ethernet interface 0/1 only:

```
Router(config)# interface ethernet 0/1
Router(config-if)# snmp ifindex persist
Router(config-if)# exit
```

In the following example, ifIndex persistence is enabled for all interfaces and then disabled for Ethernet interface 0/1 only:

```
Router(config)# snmp-server ifindex persist
Router(config)# interface ethernet 0/1
Router(config-if)# no snmp ifindex persist
Router(config-if)# exit
```

In the following example, ifIndex persistence is enabled for service instance 100 on Ethernet interface 0/1:

```
Router(config)# interface ethernet 0/1
Router(config-if)# service instance 100 ethernet
Router(config-if-srv)# snmp ifindex persist
```

Router(config-if-srv)# **exit**

Related Commands

Command	Description
snmp ifindex clear	Clears previously configured SNMP ifIndex commands for a specific interface or service instance.
snmp-server ifindex persist	Enables ifIndex values that will remain constant across reboots for use by SNMP.

snmp trap illegal-address

To issue a Simple Network Management Protocol (SNMP) trap when a MAC address violation is detected on an Ethernet hub port of a Cisco 2505, Cisco 2507, or Cisco 2516 router, use the **snmptrapillegal-address** command in hub configuration mode. To disable this function, use the **no** form of this command.

snmp trap illegal-address
no snmp trap illegal-address

Syntax Description

This command has no arguments or keywords.

Command Default

No SNMP trap is issued.

Command Modes

Hub configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

In addition to setting the **snmptrapillegal-address**command on the Ethernet hub, you can set the frequency that the trap is sent to the network management station (NMS). This is done on the NMS via the Cisco Repeater MIB. The frequency of the trap can be configured for once only or at a decaying rate (the default). If the decaying rate is used, the first trap is sent immediately, the second trap is sent after one minute, the third trap is sent after two minutes, and so on until 32 minutes, at which time the trap is sent every 32 minutes. If you use a decaying rate, you can also set the trap acknowledgment so that the trap will be acknowledged after it is received and will no longer be sent to the network management station.

Because traps are not reliable, additional information on a port basis is provided by the Cisco Repeater MIB. The network management function can query the following information: the last illegal MAC source address, the illegal address trap acknowledgment, the illegal address trap enabled, the illegal address first heard (timestamp), the illegal address last heard (timestamp), the last illegal address trap count for the port, and the illegal address trap total count for the port.

In addition to issuing a trap when a MAC address violation is detected, the port is also disabled as long as the MAC address is invalid. The port is enabled and the trap is no longer sent when the MAC address is valid (that is, either the address was configured correctly or learned).

Examples

The following example enables an SNMP trap to be issued when a MAC address violation is detected on hub ports 2, 3, or 4. SNMP support must already be configured on the router.

```
Router(config)#
 hub ethernet 0 2 4
Router(config-hub)#
 snmp trap illegal-address
```

Related Commands

Command	Description
hub	Enables and configures a port on an Ethernet hub of a Cisco 2505 or Cisco 2507 router.

snmp-server ifindex persist

Note This command is not supported in Cisco IOS Release 12.2SR. For Cisco IOS Release 12.2SR, use the **snmpifmibifindexpersist** command.

To globally enable ifIndex values that will remain constant across reboots for use by Simple Network Management Protocol (SNMP), use the **snmp-serverifindexpersist** command in global configuration mode. To globally disable ifIndex persistence, use the **no** form of this command.

snmp-server ifindex persist
no snmp-server ifindex persist

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(11)S	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was integrated into Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was replaced by the **snmpifmibifindexpersist**command in Cisco IOS Release 12.2SR.

Usage Guidelines

Interface Index Persistence means that ifIndex values in the IF-MIB persist across reboots, allowing for consistent identification of specific interfaces using SNMP.

The **snmp-serverifindexpersist** global configuration command will not override interface-specific configuration. Interface-specific configuration of ifIndex persistence is performed with the **[no]snmpifindexpersist** and **snmpifindexclear** interface configuration commands.

The **[no]snmp-serverifindexpersist** global configuration command enables and disables ifIndex persistence for all interfaces on the routing device using ifDescr and ifIndex entries in the ifIndex table of the IF-MIB.

Examples

In the following example, ifIndex persistence is enabled for all interfaces:

```
Router(config)# snmp-server ifindex persist
```

Note that in this example if ifIndex persistence was previously disabled for a specific interface using the **nosnmpifindexpersist** interface configuration command, ifIndex persistence will remain disabled for that interface. The global ifIndex command does not override the interface-specific commands.

Related Commands

Command	Description
snmp ifindex clear	Clears any previously configured snmp ifIndex commands issued in interface configuration mode for a specific interface.
snmp ifindex persist	Enables ifIndex values in the Interfaces MIB (IF-MIB) that persist across reboots (ifIndex persistence) only on a specific interface.

snr margin

To set the signal-to-noise ratio (SNR) on the controller to improve the line stability, use the **snrmargin** command in controller configuration mode. To reset the SNR to default settings, use the **no** form of this command.

snr margin {**current** [{*snr-value* | **disable**}] | **snext** [{*snr-value* | **disable**}]}
no snr margin {**current** | **snext**}

Syntax Description

current	Sets the current signal-to-noise ratio on the controller. To disable the current SNR, set **current** to **disable**.
snext	Sets the Self Near End Cross Talk (SNEXT) signal-to-noise ratio. To disable the SNEXT, set **snext** to **disable**.
snr-value	(Optional) Value, in decibels (dB), for the signal-to-noise ratio on the controller or the SNEXT. Range is from -10 to 10 . The default value is 0.
disable	(Optional) Disables the **snrmargin** command.

Command Default

The default value for both **current** and **snext** is 0.

Command Modes

Controller configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.3(4)XG	This command was integrated into Cisco IOS Release 12.3(4)XG on the Cisco 1700 series routers.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T on Cisco 2600 series, Cisco 3631, and Cisco 3700 series routers.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T on Cisco 2800 series and Cisco 3800 series routers.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T on Cisco 1800 series routers.

Usage Guidelines

The **snrmargincurrent**command can create a more stable line by making the line train more than the current noise margin plus signal-to-noise ratio threshold during training time. If any external noise is applied that is less than the set SNR margin, the line will be stable.

The **snrmarginsnext**command can create a more stable line by making the line train more than the Self Near End Cross Talk (SNEXT) threshold during training time. If any external noise is applied that is less than the set SNEXT margin, the line will be stable.

Examples

SNR with SNEXT Disabled

The following example configures the signal-to-noise ratio to 5 dB on the DSL controller in slot 3 and port 0 and disables the SNEXT signal-to-ratio.

```
Router(config)# controller
 dsl
 3/0
Router(config-controller)# snr margin
current

5
Router(config)# controller
 dsl
 3/0
Router(config-controller)# snr margin
snext

disable
```

SNR Margin set on CPE Router

The following example shows the **snrmarginsnext5** command issued on the customer premises equipment (CPE) router.

```
Router_CPE(config)# controller dsl
 1/0
Router_CPE(config-controller)# snr margin
 snext
 5
Router_CPE(config-controller)#
*Jun 15 18:29:38.511: %CONTROLLER-5-UPDOWN: Controller DSL 1/0, changed state tn
*Jun 15 18:29:40.511: %LINK-3-UPDOWN: Interface ATM1/0, changed state to down
*Jun 15 18:29:41.511: %LINEPROTO-5-UPDOWN: Line protocol on Interface ATM1/0, cn
*Jun 15 18:30:04.579:  DSL 1/0 controller Link up! line rate: 4608 Kbps
*Jun 15 18:30:04.579: %CONTROLLER-5-UPDOWN: Controller DSL 1/0, changed state tp
*Jun 15 18:30:12.351: %LINK-3-UPDOWN: Interface ATM1/0, changed state to up
*Jun 15 18:30:13.351: %LINEPROTO-5-UPDOWN: Line protocol on Interface ATM1/0, cp
```

Status on CO Side with SNR Margin set on CPE Router

The following example is the resulting output on the router that is configured as the central office (CO) side after the **snrmarginsnext5** command is entered on the CPE side.

```
Router_CO#
Jun 15 18:29:42.781: %CONTROLLER-5-UPDOWN: Controller DSL 0/0, changed state ton
Jun 15 18:29:44.784: %LINK-3-UPDOWN: Interface ATM0/0, changed state to down
Jun 15 18:29:45.786: %LINEPROTO-5-UPDOWN: Line protocol on Interface ATM0/0, chn
Jun 15 18:30:03.122:  DSL 0/0 controller Link up! line rate: 4608 Kbps
Jun 15 18:30:03.122: %CONTROLLER-5-UPDOWN: Controller DSL 0/0, changed state top
Jun 15 18:30:11.456: %LINK-3-UPDOWN: Interface ATM0/0, changed state to up
Jun 15 18:30:12.458: %LINEPROTO-5-UPDOWN: Line protocol on Interface ATM0/0, chp
```

source-address

To configure source address control on a port on an Ethernet hub of a Cisco 2505 or Cisco 2507 router, use the **source-address** command in hub configuration mode. To remove a previously defined source address, use the **no** form of this command.

source-address [*mac-address*]
no source-address

Syntax Description

mac-address	(Optional) MAC address in the packets that the hub will allow to access the network.

Command Default

Source address control is disabled.

Command Modes

Hub configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If you omit the MAC address, the hub uses the value in the last source address register, and if the address register is invalid, it will remember the first MAC address it receives on the previously specified port and allow only packets from that MAC address onto that port.

Examples

The following example configures the hub to allow only packets from MAC address 1111.2222.3333 on port 2 of hub 0:

```
Router(config)#
 hub ethernet 0 2
Router(config-hub)#
 source-address 1111.2222.3333
```

The following example configures the hub to use the value of the last source address register. If the address register is invalid, it will remember the first MAC address it receives on port 2 and allow only packets from the learned MAC address on port 2:

```
Router(config)#
 hub ethernet 0 2
Router(config-hub)#
 source-address
```

Related Commands

Command	Description
hub	Enables and configures a port on an Ethernet hub of a Cisco 2505 or Cisco 2507 router.

speed

To configure the speed for a Fast Ethernet or Gigabit Ethernet interface, use the **speed** command in interface configuration mode. To return to the default configuration, use the **no** form of this command.

speed {**10** | **100** | **1000** [**negotiate**] | **auto** [*speed-list*]}
no speed

Syntax Description

10	Configures the interface to transmit at 10 Mbps.
100	Configures the interface to transmit at 100 Mbps.
1000	Configures the interface to transmit at 1000 Mbps. This keyword is valid only for interfaces that support Gigabit Ethernet.
auto	Enables Fast Ethernet autonegotiation. The interface automatically operates at 10 Mbps or 100 Mbps depending on environmental factors, such as the type of media and transmission speeds for the peer routers, hubs, and switches used in the network configuration. Autonegotiation is the default.
negotiate	(Optional) Enables or disables the link-negotiation protocol on Gigabit Ethernet ports.
speed-list	(Optional) Speed autonegotiation capability for a specific speed; see the "Usage Guidelines" section for valid values.

Command Default

Autonegotiation is enabled. The command is set to **auto**.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.2(10)P	This command was introduced.
12.1(7)E	This command was modified. The **1000** keyword was added for Gigabit Ethernet interfaces.
12.2S	This command was integrated into Cisco IOS Release 12.2 S.
12.2(20)S2	This command was implemented on the 4-port 10/100 Fast Ethernet SPA and the 2-port 10/100/1000 Gigabit Ethernet SPA on the Cisco 7304 router.
12.2(14)SX	This command was implemented on the Supervisor Engine 720.
12.2(17a)SX	This command was modified. The *speed-list* argument was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S.

Release	Modification
15.2(02)SA	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

Use the **speed** {**10** | **100**} command for 10/100 ports, the **speed auto 10 100 1000** command for 10/100/1000 ports, and the **speed 1000** [**negotiate**] command for Gigabit Ethernet ports.

Cisco Cloud Services Router 1000V Series

Cisco Cloud Services Router 1000V Series does not support the **speed** command.

Cisco 7600 Series Routers

Cisco 7600 Series Routers cannot automatically negotiate interface speed and duplex mode if either of the connecting interfaces is configured to a value other than **auto**.

Ethernet Interfaces

If you set the Ethernet interface speed to **auto** on a 10/100-Mbps or 10/100/1000-Mbps Ethernet interface, both duplex operation and speed are autonegotiated.

Gigabit Ethernet Interfaces

The Gigabit Ethernet interfaces are full duplex only. You cannot change the duplex mode on Gigabit Ethernet interfaces or on a 10/100/1000-Mbps interface that is configured for Gigabit Ethernet.

SPA Interfaces

The **speed** command applies to Shared Port Adapter (SPA) interfaces that use RJ-45 media. Gigabit Ethernet interfaces using fiber media support 1000-Mbps speed only and use the **negotiation** command to enable and disable autonegotiation.

See also “Flow Control” in the “Usage Guidelines” section.

Speed Command Syntax Combinations

The table below lists the supported command options by interface.

Table 278: Supported speed Command Options

Interface Type	Supported Syntax	Default Settings	Usage Guidelines
10/100-Mbps module	**speed** {**10** | **100**} **speed auto 10 100**	**auto**	If the speed is set to **auto**, you cannot set **duplex**. If the speed is set to **10** or **100**, without configuring the duplex setting, the duplex is set to **half** by default.

Interface Type	Supported Syntax	Default Settings	Usage Guidelines
10/100/1000-Mbps interface	**speed auto 10 100 1000**	**auto**	If the speed is set to **auto**, you cannot set **duplex**. If the speed is set to **10** or **100**, without configuring the duplex setting, the duplex is set to **half** by default. If the speed is set to **10** or **100**, the interface is not forced to half duplex by default.
100-Mbps fiber modules	Factory set	Not applicable.	
Gigabit Ethernet module	**speed 1000** [**negotiate**]	Speed is 1000 or negotiation is enabled.	Speed, duplex, flow control, and clocking negotiations are enabled.
10-Mbps ports	Factory set	Not applicable.	

Autonegotiation

To enable the autonegotiation capability on an RJ-45 interface, you must set either the **speed** command or the **duplex** command to **auto**. The default configuration is that both commands are set to **auto**.

If you need to force an interface port to operate with certain settings and, therefore, disable autonegotiation, you must be sure that the remote link is configured for compatible link settings for proper transmission including support of flow control on the link.

When you enable link negotiation, the speed, duplex, flow control, and clocking negotiations between two Gigabit Ethernet ports are automatically enabled.

Flow Control

Flow control support is always advertised when autonegotiation is enabled.

Every interface on a 4-port 10/100 Fast Ethernet SPA supports transmission of pause frames to stop packet flow when the Modular Services Card (MSC) is full. You cannot disable flow control for an interface on the 4-port 10/100 Fast Ethernet SPA. Therefore, flow control support is not configurable, but it is advertised during autonegotiation.

If you disable autonegotiation, then you must be sure that the remote device is configured to support flow control because flow control is automatically enabled for all interfaces on the 4-port 10/100 Fast Ethernet SPA.

Speed Settings

Separate the *speed-list* entries with a space.

When manually configuring the interface speed to either 10 or 100 Mbps, the switch prompts you to configure duplex mode on the interface.

The following *speed-list* configurations are supported:

- **speed auto**—Negotiate all speeds.
- **speed auto 10 100**—Negotiate 10 and 100 speeds only.
- **speed auto 10 100 1000**—Negotiate all speeds.

Speed and Duplex Combinations

The table below describes the interface behavior for various combinations of the **duplex** and **speed** command settings. The specified **duplex** command configured with the specified **speed** command produces the resulting system action.

If you decide to configure the interface speed and duplex commands manually, and enter a value other than **speed auto** (for example, 10 or 100 Mbps), ensure that you configure a connected interface with a matching speed using the speed command without using the **auto** keyword.

If you specify both a **duplex** and **speed** setting other than **auto** on an RJ-45 interface, then autonegotiation is disabled for the interface.

You cannot set the duplex mode to **half** when the port speed is set to **1000**, and similarly, you cannot set the port speed to **1000** when the mode is set to **half duplex**. In addition, if the port speed is set to **auto**, the **duplex** command is rejected.

Caution Changing the interface speed and duplex mode might shut down and reenable the interface during reconfiguration.

Table 279: Relationship Between duplex and speed Commands

duplex Command	speed Command	Resulting System Action
duplex auto	**speed auto**	Autonegotiates both speed and duplex settings. The interface advertises the capability for the following link settings: • 10 Mbps and half duplex • 10 Mbps and full duplex • 100 Mbps and half duplex • 100 Mbps and full duplex • 1000 Mbps and half duplex (Gigabit Ethernet only) • 1000 Mbps and full duplex (Gigabit Ethernet only)

duplex Command	speed Command	Resulting System Action
duplex auto	**speed 10** or **speed 100** or **speed 1000**	Autonegotiates the duplex mode. The interface advertises the capability for both half-duplex and full-duplex modes at the configured speed. For example, if the **speed 100** command is configured with **duplex auto**, then the interface advertises the following capability: • 100 Mbps and half duplex • 100 Mbps and full duplex
duplex half or **duplex full**	**speed auto**	Autonegotiates the speed. The interface advertises the capability for duplex mode for Fast Ethernet interfaces at a speed of 10-Mbps and 100-Mbps, and Gigabit interfaces at 10-Mbps, 100-Mbps, and 1000-Mbps. For example, if the **duplex full** command is configured with the **speed auto** command, then the interface advertises the following capability: • 10 Mbps and full duplex • 100 Mbps and full duplex • 1000 Mbps and full duplex (Gigabit Ethernet interfaces only)
duplex half	**speed 10**	Forces a speed of 10-Mbps and the half-duplex operation, and disables autonegotiation on the interface.
duplex full	**speed 10**	Forces a speed of10-Mbps and the full-duplex operation, and disables autonegotiation on the interface.
duplex half	**speed 100**	Forces a speed of 100-Mbps and the half-duplex operation, and disables autonegotiation on the interface.
duplex full	**speed 100**	Forces a speed of 100-Mbps and the full-duplex operation, and disables autonegotiation on the interface.
duplex half	**speed 1000**	Forces a speed of 1000-Mbps and the half-duplex operation, and disables autonegotiation on the interface (Gigabit Ethernet only).
duplex full	**speed 1000**	Forces a speed of 1000-Mbps and the full-duplex operation, and disables autonegotiation on the interface (Gigabit Ethernet only).

Examples

The following example specifies the advertisement of only the 10 Mbps operation and either the full-duplex or half-duplex capability during autonegotiation for the second interface (port 1) on the SPA located in the bottom subslot (1) of the MSC that is installed in slot 2 of the Cisco 7304 router:

```
Device# configure terminal
Device(config)# interface fastethernet 2/1/1
Device(config-if)# speed 10
Device(config-if)# duplex auto
```

With this configuration, the interface advertises the following capabilities during autonegotiation:

- 10 Mbps and half duplex
- 10 Mbps and full duplex

Related Commands

Command	Description
duplex	Configures the duplex operation on an interface.
interface fastethernet	Selects a particular Fast Ethernet interface for configuration.
interface gigabitethernet	Selects a particular Gigabit Ethernet interface for configuration.
show controllers fastethernet	Displays Fast Ethernet interface information, transmission statistics and errors, and the applicable MAC destination address and VLAN filtering tables.
show controllers gigabitethernet	Displays Gigabit Ethernet interface information, transmission statistics and errors, and the applicable MAC destination address and VLAN filtering tables.
show interfaces fastethernet	Displays information about the Fast Ethernet interfaces.
show interfaces gigabitethernet	Displays information about the Gigabit Ethernet interfaces.

squelch

To extend the Ethernet twisted-pair 10BASE-T capability beyond the standard 100 meters on the Cisco 4000 platform, use the **squelch** command in interface configuration mode. To restore the default, use the **no** form of this command.

squelch {**normal** | **reduced**}
no squelch

Syntax Description

normal	Allows normal capability. This is the default.
reduced	Allows extended 10BASE-T capability.

Command Default

Normal range

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example extends the twisted-pair 10BASE-T capability on the cable attached to Ethernet interface 2:

```
Router(config
)
# interface ethernet 2
Router(config
-if)
# squelch reduced
```

sra line

To accommodate changes to the total link capacity with the least amount of disruption to communications, use the **sra line** command in controller configuration mode. To disable seamless rate adaptation, use the **no** form of this command.

sra [line *line-number***]**
no sra [line *line-number***]**

Syntax Description

line-number	Line number. Valid values are either 0 or 1.

Command Default

Seamless rate adaptation is disabled.

Command Modes

Controller configuration (config-controller)#

Command History

Release	Modification
15.4(4)T	This command was introduced.

Usage Guidelines

If you specify the line-number, seamless rate adaptation will be enabled only on that line. If you do not specify the line-number, SRA will be enabled on both the lines.

Examples

The following example shows how to enable seamless rate adaptation on line 0:

```
Router(config-controller)# sra line 0
```

The following example shows how to disable seamless rate adaptation:

```
Router(config-controller)# no sra
```

Related Commands

Command	Description
bitswap line	Diverts the data of a disturbed transmission channel to other channels.

standby port

To defer the activation of a port on the standby chassis during standby recovery, use the **standbyport** virtual switching system (VSS) mode command. To disable port deferral activation, use the **no** form of this command.

standby port {**bringup** *num duration* | **delay** *seconds*}

Syntax Description

bringup	Configures the number of ports to be activated per cycle and the waiting time between cycles. Note: You must configure the standby port delay time before you can configure the standby port bringup time.
num	Number of ports to be activated per cycle. Range: 1 to 100. Default: 1.
duration	Period of time in seconds between cycles. Range: 1 to 10. Default: 1.
delay *seconds*	Specifies the period in seconds before port activation is performed. Range: 30 to 3600. Default: 0.

Command Default

Port deferral activation is disabled if standby port delay is not configured. If port deferral activation is enabled, the default number of ports activated in one cycle is one and the duration of the cycle is one second.

Command Modes

Virtual switch configuration submode (config-vs-domain)

Command History

Release	Modification
12.2(33)SXH2	Support for this command was introduced.

Usage Guidelines

Note We recommend that enter you this command under TAC supervision.

Note You must configure the standby port delay command before you can configure the standby port bringup command.

If the you configure the standby port bringup without configuring the standby port delay, a message is displayed asking you to configure the standby port delay first and then the standby port bringup. If you remove the standby port delay configuration, the standby port bringup is automatically removed.

In default configuration, all ports are activated simultaneously when a failed chassis is restarted as the standby chassis. You can enter the **standbyport** command to defer the activation of ports that are not virtual switch link (VSL) ports and then activate the ports in groups over a period of time.

You can enter the **standbyport** command to defer the activation of ports that are not virtual switch link (VSL) ports and then activate the ports in groups over a period of time. This can help in reducing traffic loss on the standby ports and alleviate the high CPU utilization on the active switch and route processors during system initialization of the standby chassis.

Examples

The following example shows how to configure the period in seconds before port activation is performed:

```
Router(config)# switch virtual domain 22
Router (config-vs-domain)# standby port delay 400
Router (config-vs-domain)#
```

The following example shows how to configure the bringup delay for a port’s activation during a standby recovery:

```
Router(config)# switch virtual domain 22
Router (config-vs-domain)# standby port bringup 2 30
Router (config-vs-domain)#
```

Related Commands

Command	Description
switch virtual domain	Assigns a switch number and enters virtual switch domain configuration submode.

sts-1

To configure the Synchronous Transport Signal (STS) (level)-1 in the SONET hierarchy, use the **sts-1** command in controller configuration mode.

sts-1 *number*

Syntax Description

number	Specifies the sts-1 number. The range is 1 to 3.

Command Default

None

Command Modes

Controller configuration

Command History

Release	Modification
15.1(01)S	This command was introduced on the Cisco 7600 routers.
Cisco IOS XE Everest 16.5.1	This command was introduced on the Cisco ASR 920 Routers and Cisco NCS 4200 Series.

Examples

This example shows how to configure the (STS) (level)-1:

```
Router(config)# controller sonet-acr 1
Router(config-controller)#
sts-1 2
```

Related Commands

Command	Description
vtg	Configures the (CESoPSN) CEM group.
mode vt-15	Configures the path operation mode.
controller sonet-acr	Configures the SONET Access Circuit Redundancy (ACR) virtual controller.

squelch through system jumbomtu

squelch

To extend the Ethernet twisted-pair 10BASE-T capability beyond the standard 100 meters on the Cisco 4000 platform, use the **squelch** command in interface configuration mode. To restore the default, use the **no** form of this command.

squelch {**normal** | **reduced**}
no squelch

Syntax Description

normal	Allows normal capability. This is the default.
reduced	Allows extended 10BASE-T capability.

Command Default

Normal range

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example extends the twisted-pair 10BASE-T capability on the cable attached to Ethernet interface 2:

```
Router(config
)
# interface ethernet 2
Router(config
-if)
# squelch reduced
```

srp buffer-size

To make adjustments to buffer settings on the receive side for different priority traffic, use the **srpbuffer-size**command in interface configuration mode. To disable buffer size configurations, use the **no** form of this command.

srp buffer-size receive [{**low** *buffer* | **medium** *buffer* | **high** *buffer*}]
no srp buffer-size receive [{**low** *buffer* | **medium** *buffer* | **high** *buffer*}]

Syntax Description

receive	Allocates SDRAM buffer for incoming packets.
low *buffer*	(Optional) Specifies buffer size, in kilobytes, for low-priority packets. Any number from 16 to 8192. The default is 8192.
medium *buffer*	(Optional) Specifies buffer size, in kilobytes, for medium-priority packets. Any number from 16 to 8192. The default is 4096.
high *buffer*	(Optional) Specifies buffer size, in kilobytes, for high-priority packets. Any number from 16 to 8192. The default is 4096.

Command Default

low = 8192 kilobytes, medium = 4096 kilobytes, high = 4096 kilobytes

Command Modes

Interface configuration

Command History

Release	Modification
12.0(6)S	This command was introduced.
12.0(7)XE1	This command was implemented on Cisco 7500 series routers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example sets the buffer size for the receive side at the high setting of 17 kilobytes:

```
Router(config-if)# srp buffer-size receive high 17
```

Related Commands

Command	Description
mtu	Adjusts the maximum packet size MTU size.
srp deficit-round-robin	Transfers packets from the internal receive buffer to Cisco IOS software.

srp deficit-round-robin

To transfer packets from the internal receive buffer to Cisco IOS software, use the **srpdeficit-round-robin** command in interface configuration mode. To disable the packet transfer, use the **no** form of this command.

srp deficit-round-robin [{**input** | **output**}] [{**low** | **medium** | **high**}] [{**quantum** *number* | **deficit** *number*}]
no srp deficit-round-robin

Syntax Description

input	(Optional) Specifies input buffer.
output	(Optional) Specifies output buffer.
low	(Optional) Specifies low-priority queue level.
medium	(Optional) Specifies medium-priority queue level.
high	(Optional) Specifies high-priority queue level.
quantum *number*	(Optional) Specifies the Deficit Round Robin (DRR) quantum value. Any number from 9216 to 32767. The default is 9216.
deficit *number*	(Optional) Specifies the DRR deficit value. Any number from 0 to 65535. The default is 16384.

Command Default

quantum : 9216**deficit**: 16384

Command Modes

Interface configuration

Command History

Release	Modification
12.0(6)S	This command was introduced.
12.0(7)XE1	This command was implemented on Cisco 7500 series routers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to configure packets for the medium-priority input queue:

```
Router(config)# srp deficit-round-robin input medium deficit 15000
```

Related Commands

Command	Description
srp buffer-size	Makes adjustments to buffer settings on the receive side for different priority traffic.

Command	Description
srp priority-map	Sets priority mapping for transmitting and receiving packets.
srp random-detect	Configures WRED parameters on packets received through an SRP interface.

srp loopback

To loop the spatial reuse protocol (SRP) interface on an OC-12c DPTIP, use the **srploopback**command in interfaceconfiguration mode. To remove the loopback, use the **no** form of this command.

srp loopback {**internal** | **line**} {**a** | **b**}
no srp loopback

Syntax Description

internal	Sets the loopback toward the network before going through the framer
line	Loops the payload data toward the network.
a	Loops back the A side of the interface (inner tx, outer rx).
b	Loops back the B side of the interface (outer tx, inner rx).

Command Default

No loops are configured.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(6)S	This command was introduced.
12.0(7)XE1	This command was introduced on Cisco 7500 series routers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command for troubleshooting purposes.

Examples

The following example configures the loopback test on the A side of the SRP interface:

```
Router(config-if)# srp loopback line a
```

srp priority-map

To set priority mapping for transmitting and receiving packets, use the**srppriority-map**command in interface configuration mode. To disable priority mapping u se the **no** form of this command .

srp priority-map receive {**low** *priority* | **medium** *priority* | **high** *priority* | **transmit** {**medium** *priority* | **high** *priority*}}
no srp priority-map

Syntax Description

receive	Specifies priority mapping for receiving packets.
transmit	Specifies priority mapping for transmitting packets.
low *priority*	(Optional) Specifies mapping for low-priority packets. Any number from 1 to 8. The default is 1.
medium *buffer*	(Optional) Specifies mapping for medium-priority packets. Any number from 1 to 8. The default is 3.
high *buffer*	(Optional) Specifies mapping for high-priority packets. Any number from 1 to 8. The default is 5 for receiving packets, and default is 7 for transmitting packets.

Command Default

receive low : 1**receivemedium**: 3 **receivehigh**: 5 **transmithigh**: 7

Command Modes

Interface configuration

Command History

Release	Modification
12.0(6)S	This command was introduced.
12.0(7)XE1	This command was implemented on Cisco 7500 series routers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The spatial reuse protocol (SRP) interface provides commands to enforce quality of service (QoS) functionality on the transmit side and receive side of Cisco routers. SRP uses the IP type of service (ToS) field values to determine packet priority.

The SRP interface classifies traffic on the transmit side into high- and low-priority traffic. High-priority traffic is rate shaped and has higher priority than low-priority traffic. You have the option to configure high- or low-priority traffic and can rate limit the high-priority traffic.

The **srppriority-maptransmit** command enables the user to specify IP packets with values equal to or greater than the ToS value to be considered as high-priority traffic.

On the receive side, when WRED is enabled, SRP hardware classifies packets into high-, medium-, and low-priority packets on the basis of the IP ToS value. After classification, it stores the packet into the internal receive buffer. The receive buffer is partitioned for each priority packet. Cisco routers can employ WRED on the basis of the IP ToS value. Routers also employ the Deficit Round Robin (DRR) algorithm to transfer packets from the internal receive buffer to Cisco IOS software.

The **srppriority-mapreceive** command enables the user to classify packets as high, medium, or low based on the IP ToS value.

Examples

The following example configures Cisco 7500 series routers to transmit packets with priority greater than 5 as high-priority packets:

```
Router(config-if)# srp priority-map transmit high 6
```

Related Commands

Command	Description
srp random-detect	Configures WRED parameters on packets received through an SRP interface.

srp random-detect

To configure weighted RED (WRED) parameters on packets received through an spatial reuse protocol (SRP) interface, use the **srprandom-detect**command in interfaceconfiguration mode. To return the value to the default, use the **no** form of this command.

srp random-detect {**compute-interval** *interval* | **enable** | **input** [{**low** | **medium** | **high**}] | [{**exponential-weight** *weight* | **precedence** *precedence*}]}
no srp random-detect

Syntax Description

compute-interval *compute-interval*	Specifies the queue depth compute interval, in nanoseconds. Number in the range from 1 to 128. Default is 128.
enable	Enables WRED.
input	Specifies WRED on packet input path.
low	(Optional) Specifies low-priority queue level.
medium	(Optional) Specifies medium-priority queue level.
high	(Optional) Specifies high-priority queue level.
exponential-weight *weight*	(Optional) Specifies the queue weight, in bits. Number in the range from 0 to 6. The default is 6.
precedence *number*	(Optional) Specifies the input queue precedence. Number in the range from 0 to 7. The default is 7.

Command Default

compute-interval: 128 weight: 6 precedence: 7

Command Modes

Interface configuration

Command History

Release	Modification
12.0(6)S	This command was introduced.
12.0(7)XE1	This command was implemented on Cisco 7500 series routers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example configures WRED parameters on packets received through an SRP interface with a weight factor of 5:

```
Router(config-if)# srp random-detect input high exponential-weight 5
```

srp shutdown

To disable the spatial reuse protocol (SRP) interface, use the **srpshutdown** command in interface configuration mode. To restart a disabled interface, use the **no** form of this command.

srp shutdown [{**a** | **b**}]
no srp shutdown [{**a** | **b**}]

Syntax Description

a	(Optional) Specifies side A of the SRP interface.
b	(Optional) Specifies side B of the SRP interface.

Command Default

The SRP interface continues to be enabled until this command is issued.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(6)S	This command was introduced.
12.0(7)XE1	This command was introduced on Cisco 7500 series routers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **srpshutdown** command disables all functions on the specified side.

Examples

The following example turns off side A of the SRP interface:

```
Router(config-if)# srp shutdown a
```

srp tx-traffic-rate

To limit the amount of high-priority traffic that the spatial reuse protocol (SRP) interface can handle, use the**srptx-traffic-rate** command in interface configuration mode. Use the **no** form of this command to disable transmitted traffic rate .

srp **tx-traffic-rate** *number*
no **srp** **tx-traffic-rate** *number*

Syntax Description

number	Transmission speed, in kilobits per second. The range is from 1 to 65535. Default is 10.

Command Default

number : 10

Command Modes

Interface configuration

Command History

Release	Modification
12.0(6)S	This command was introduced.
12.0(7)XE1	This command was implemented on Cisco 7500 series routers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example configures SRP traffic to transmit at 1000 kilobits per second:

```
Router(config-if)# srp tx-traffic-rate 1000
```

stack-mib portname

To specify a name string for a port, use the **stack-mib portname**command in interface configuration mode.

stack-mib portname *portname*

Syntax Description

portname	Name for a port.

Command Default

This command has no default settings.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2917d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Using the **stack-mib** command to set a name string to a port corresponds to the portName MIB object in the portTable of CISCO-STACK-MIB. portName is the MIB object in the portTable of CISCO-STACK-MIB. You can set this object to be descriptive text describing the function of the interface.

Examples

This example shows how to set a name to a port:

```
Router(config-if)#
stack-mib portname portall
Router(config-if)#
```

storm-control

To enable broadcast, multicast, or unicast storm control on a port or to specify the action when a storm occurs on a port, use the **storm-control** command in interface configuration mode. To disable storm control for broadcast, multicast, or unicast traffic or to disable the specified storm-control action, use the **no** form of this command.

storm-control {{**broadcast** | **multicast** | **unicast**} **level** *level* | **action** {**shutdown** | **trap**}}
no storm-control {{**broadcast** | **multicast** | **unicast**} **level** | **action** {**shutdown** | **trap**}}

Cisco ME 2600X Series Ethernet Access Switch
storm-control {{**broadcast** | **multicast**} **cir** *cir-value* | **action shutdown**}
no storm-control {{**broadcast** | **multicast**} **cir** *cir-value* | **action shutdown**}

Syntax Description

broadcast	Enables broadcast storm control on the port.
multicast	Enables multicast storm control on the port.
unicast	Enables unicast storm control on the port.
level *level*	Defines the rising and falling suppression levels. • *level* —Rising suppression level as a percent of the total bandwidth (up to two decimal places). The valid values are from 0 to 100. When the value specified for a level is reached, the flooding of storm packets is blocked.
action	Specifies the action to take when a storm occurs on a port. The default action is to filter traffic.
shutdown	Disables the port during a storm.
trap	Sends a Simple Network Management Protocol (SNMP) trap.
cir *cir-value*	Defines the Committed Information Rate (cir). • *cir-value*—The acceptable range is 10000000 -1000000000 for a gigabit ethernet interface, and 100000000-10000000000 for a ten gigabit interface. The recommended maximum value is up to 98 percent.

Command Default

Broadcast, multicast, and unicast storm control is disabled. The default action is to filter traffic.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(2)XT	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T to support switchport creation.

Release	Modification
12.2(15)ZJ	This command was integrated into Cisco IOS Release 12.2(15)ZJ. The **level** *level* keyword-argument pair, and the **action** and **shutdown** keywords were added.
15.0(1)S	This command was modified. The **trap** keyword was added.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
15.2(02)SA	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

Use the **storm-control** command to enable or disable broadcast, multicast, or unicast storm control on a port. After a port is disabled during a storm, use the **no shutdown** interface configuration command to enable the port.

The suppression levels are entered as a percentage of total bandwidth. A suppression value of 100 percent means that no limit is placed on the specified traffic type. This command is enabled only when the rising suppression level is less than 100 percent. If no other storm-control configuration is specified, the default action is to filter the traffic that is causing the storm.

When a storm occurs and the action is to filter traffic, and the falling suppression level is not specified, the networking device blocks all traffic until the traffic rate drops below the rising suppression level. If the falling suppression level is specified, the networking device blocks traffic until the traffic rate drops below this level.

When a multicast or unicast storm occurs and the action is to filter traffic, the networking device blocks all traffic (broadcast, multicast, and unicast traffic) and sends only Spanning Tree Protocol (STP) packets.

When a broadcast storm occurs and the action is to filter traffic, the networking device blocks only broadcast traffic.

The trap action is used to send an SNMP trap when a broadcast storm occurs.

Note Adding or removing of storm control configuration under the member link of LACP is not supported.

Note On Cisco Catalyst 3750 Series Switches, when the **storm-control** command is applied, it is rejected and the port is not put into a suspended state.

Examples

The following example shows how to enable broadcast storm control on a port with a 75.67-percent rising suppression level:

```
Device(config-if)# storm-control broadcast level 75.67
```

The following example shows how to enable multicast storm control on a port with an 87-percent rising suppression level:

```
Device(config-if)# storm-control multicast level 87
```

The following example shows how to enable the shutdown action on a port:

```
Device(config-if)# storm-control action shutdown
```

The following example shows how to disable the shutdown action on a port:

```
Device(config-if)# no storm-control action shutdown
```

The following example shows how to enable the trap action on a port:

```
Device(config-if)# storm-control action trap
```

The following example shows how to disable the trap action on a port:

```
Device(config-if)# no storm-control action trap
```

Related Commands

Command	Description
no shutdown	Enables a port.
show storm-control	Displays the packet-storm control information.
shutdown (interface)	Disables an interface.

storm-control level

To set the suppression level, use the **storm-control level** command in interface configuration mode. To turn off the suppression mode, use the **no** form of this command.

storm-control {**broadcast** | **multicast** | **unicast**} **level** *level* [**.** *level*]
no storm-control {**broadcast** | **multicast** | **unicast**} **level**

Syntax Description

broadcast	Specifies the broadcast traffic.
multicast	Specifies the multicast traffic.
unicast	Specifies the unicast traffic.
level	Integer-suppression level; valid values are from 0 to 100 percent.
. *level*	(Optional) Fractional-suppression level; valid va lues are from 0 to 99.

Command Default

All packets are passed.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You can enter this command on switch ports and router ports.

Enter the **storm-control level** command to enable traffic storm control on the interface, configure the traffic storm-control level, and apply the traffic storm-control level to all traffic storm-control modes that are enabled on the interface.

Only one suppression level is shared by all three suppression modes. For example, if you set the broadcast level to 30 and set the multicast level to 40, both levels are enabled and set to 40.

The Cisco 7600 series router supports storm control for multicast and unicast traffic only on Gigabit Ethernet LAN ports. The switch supports storm control for broadcast traffic on all LAN ports.

The **multicast** and **unicast** keywords are supported on Gigabit Ethernet LAN ports only. These keywords are not supported on 10 Mbps, 10/100 Mbps, 100 Mbps, or 10-Gigabit Ethernet modules.

The period is required when you enter the fractional-suppression level.

The suppression level is entered as a percentage of the total bandwidth. A threshold value of 100 percent means that no limit is placed on traffic. A threshold value of 0 or 0.0 (fractional) percent means that all specified traffic is blocked on a port, with the following guidelines:

- A fractional level value of 0.33 or lower is the same as 0.0 on the following modules:

- WS-X6704-10GE
- WS-X6748-SFP
- WS-X6724-SFP
- WS-X6748-GE-TX

- A fractional level value of 0.29 or lower is the same as 0.0 on the WS-X6716-10G-3C / 3CXL in Oversubscription Mode.
- Enter 0 on all other modules to block all specified traffic on a port.

Enter the **show interfaces counters broadcast** command to display the discard count.

Enter the **show running-config** command to display the enabled suppression mode and level setting.

To turn off suppression for the specified traffic type, you can do one of the following:

- Set the *level* to 100 percent for the specified traffic type.
- Use the **no** form of this command.

Examples

This example shows how to enable and set the suppression level:

```
Router(config-if)#
storm-control broadcast level 30
```

This example shows how to disable the suppression mode:

```
Router(config-if)#
no storm-control multicast level
```

Related Commands

Command	Description
show interfaces counters	Displays the traffic that the physical interface sees.
show running-config	Displays the status and configuration of the module or Layer 2 VLAN.

subslot

To add an IPSec VPN SPA to a Blade Failure Group, use the **subslot** command in redundancy-linecard configuration mode.

subslot *slot* *subslot*

Syntax Description

slot	Chassis slot number. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide.
subslot	Secondary slot number on the SIP where the SPA is installed.

Command Default

No default behavior or values.

Command Modes

Redundancy-linecard configuration

Command History

Release	Modification
12.2(18)SXE2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

To complete the configuration of a Blade Failure Group, you must repeat the **subslot** command for each IPSec VPN SPA in the group.

Examples

The following example configures a Blade Failure Group that has a group ID of 1 and consists of two IPSec VPN SPAs--one IPSec VPN SPA is in slot 5, subslot 1 and one IPSec VPN SPA is in slot 6, subslot 1:

```
Router(config)# redundancy
Router
(config-red)# linecard-group 1 feature-card
Router(config-r-lc)# subslot 5/1
Router(config-r-lc)# subslot 6/1
```

Related Commands

Command	Description
linecard-group feature card	Assigns a group ID to a Blade Failure Group.
redundancy	Enters redundancy configuration mode.
show redundancy linecard-group	Displays the components of a Blade Failure Group.

switchport

Cisco 3550, 4000, and 4500 Series Switches

To put an interface that is in Layer 3 mode into Layer 2 mode for Layer 2 configuration, use the **switchport** command in interface configuration mode. To put an interface into Layer 3 mode, use the **no** form of this command.

switchport
no switchport

Cisco Catalyst 6500 and 6000 Series Switches and Cisco 7600 Series Routers

To modify the switching characteristics of the Layer 2-switched interface, use the **switchport** command (without keywords). Use the **no** form of this command (without keywords) to return the interface to the routed-interface status and cause all further Layer 2 configuration to be erased. Use the **switchport** commands (with keywords) to configure the switching characteristics.

switchport
switchport {**host** | **nonegotiate**}
no switchport
no switchport nonegotiate

Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers

To configure the server module to communicate with the router over a high-speed Multi Gigabit Fabric (MGF) backplane switch port, use the **switchport** command (with keywords) in interface configuration mode.

switchport {**access** | **mode** | **trunk**}

Cisco 1000 Series Integrated Services Routers with 4 or 8 Front-Panel Switch Ports

To configure the flex Layer 2 and Layer 3 ports to Layer 2 interface, use the **switchport** command (without keywords). To configure to Layer 3 interface, use the **no switchport** command (without keywords).

switchport
no switchport

Syntax Description

Cisco 3550, 4000, and 4500 Series Switches

This command has no arguments or keywords.

Cisco Catalyst 6500 and 6000 Series Switches and Cisco 7600 Series Routers

Table 280: Syntax Description for Cisco Catalyst 6500 and 6000 Series Switches and Cisco 7600 Series Routers

host	Optimizes the port configuration for a host connection.
nonegotiate	Specifies that the device will not engage in negotiation protocol on this interface.

Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers

Table 281: Syntax Description for Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers

access	Sets the access mode characteristics of the interface.
mode	Sets the interface type: Access or Trunk.
trunk	Sets trunk characteristics when the interface is in Trunk mode. This is the default mode.

Cisco 1000 Series Integrated Services Routers with 4 or 8 Front-Panel Switch Ports

This command has no arguments or keywords.

Command Default

Cisco 3550, 4000, and 4500 Series Switches

All interfaces are in Layer 2 mode.

Catalyst 6500/6000 Series Switches and 7600 Series Routers

The default access VLAN and trunk-interface native VLAN are default VLANs that correspond to the platform or interface hardware.

Cisco 1000 Series Integrated Services Routers with 4 or 8 Front-Panel Switch Ports

The last two ports of the front-panel switch ports (flex ports) are set to Layer 2 interface by default.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(15)ZJ	This command was implemented on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
15.1(2)T	Support for IPv6 was added.
Cisco IOS XE Release 3.9S	This command was implemented on Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Routers (ISR).
Cisco IOS XE Release 17.11.1a	This command was implemented to provide flex support on the last two Layer 2 switch ports of the Cisco 1000 Series ISRs with 4 or 8 Front-Panel Switch Ports.

Usage Guidelines

Cisco 3550, 4000, and 4500 Series Switches

Use the **no switchport** command to put the interface into the routed-interface status and to erase all Layer 2 configurations. You must use this command before assigning an IP address to a routed port. Entering the **no switchport** command shuts down the port and then reenables it, which might generate messages on the device to which the port is connected.

You can verify the switchport status of an interface by entering the **show running-config** privileged EXEC command.

Cisco Catalyst 6500 and 6000 Series Switches and Cisco 7600 Series Routers

You must enter the **switchport** command without any keywords to configure the LAN interface as a Layer 2 interface before you can enter additional **switchport** commands with keywords. This action is required only if you have not entered the **switchport** command for the interface.

Entering the **no switchport** command shuts down the port and then reenables it. This action may generate messages on the device to which the port is connected.

To optimize the port configuration, entering the **switchport host** command sets the switch port mode to access, enables spanning tree PortFast, and disables channel grouping. Only an end station can accept this configuration.

Because spanning-tree PortFast is enabled, you should enter the **switchport host** command only on ports that are connected to a single host. Connecting other Cisco 7600 series routers, hubs, concentrators, switches, and bridges to a fast-start port can cause temporary spanning-tree loops.

Enable the **switchport host** command to decrease the time that it takes to start up packet forwarding.

The no form of the **switchport** nonegotiate command removes nonegotiate status.

When using the **nonegotiate** keyword, Dynamic Inter-Switch Link Protocol and Dynamic Trunking Protocol (DISL/DTP)-negotiation packets are not sent on the interface. The device trunks or does not trunk according to the mode parameter given: access or trunk. This command returns an error if you attempt to execute it in dynamic (auto or desirable) mode.

You must force a port to trunk before you can configure it as a SPAN-destination port. Use the **switchport nonegotiate** command to force the port to trunk.

Examples

Cisco 3550, 4000, and 4500 Series Switches

The following example shows how to cause an interface to cease operating as a Layer 2 port and become a Cisco-routed (Layer 3) port:

```
Router(config-if)#no switchport
```

Cisco Catalyst 6500 and 6000 Series Switches and Cisco 7600 Series Routers

The following example shows how to cause the port interface to stop operating as a Cisco-routed port and convert to a Layer 2-switched interface:

```
Router(config-if)#
switchport
Router(config-if)#
```

Note The **switchport** command is not used on platforms that do not support Cisco-routed ports. All physical ports on such platforms are assumed to be Layer 2-switched interfaces.

The following example shows how to optimize the port configuration for a host connection:

```
Router(config-if)# switchport host
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled
Router(config-if)#
```

This example shows how to cause a port interface that has already been configured as a switched interface to refrain from negotiating trunking mode and act as a trunk or access port (depending on the mode set):

```
Router(config-if)#
switchport nonegotiate
Router(config-if)#
```

The following example shows how to cause an interface to cease operating as a Cisco-routed port and to convert it into a Layer 2 switched interface:

```
Router(config-if)#
switchport
```

Note The **switchport** command is not used on platforms that do not support Cisco-routed (Layer 3) ports. All physical ports on such platforms are assumed to be Layer 2 switched interfaces.

Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers

The following example shows how to set the interface to **access** mode:

```
Router#configure terminal
Router(config)# interface ucse 1/0/0
Router(config-if)# switchport mode access
```

The following example shows how to set the interface to **trunk** mode:

```
Router#configure terminal
Router(config)# interface ucse 1/0/0
Router(config-if)# switchport mode trunk
```

Cisco 1000 Series Integrated Services Routers with 4 or 8 Front-Panel Switch Ports

The following example shows how to convert a flex port to a Layer 3 port:

```
Device# configure terminal
Device(config)# interface GigabitEthernet 0/1/6
```

```
Device(config-if)# no switchport
Device(config-if)# ip address 10.10.0.1 255.255.255.0
Device(config-if)# exit
```

The following example shows how to convert a flex port to a Layer 2 port:

```
Device# configure terminal
Device(config)# interface GigabitEthernet 0/1/6
Device(config-if)# switchport
Device(config-if)# switchport mode access
Device(config-if)# exit
```

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
show running-config	Displays the current operating configuration.
switchport access vlan	Sets the VLAN when the interface is in Access mode.
switchport mode	Sets the interface type: Access or Trunk
switchport trunk	Sets trunk characteristics when the interface is in Trunk mode.

switchport access vlan

To set the VLAN when the interface is in access mode, use the **switchport access vlan** command in interface configuration or template configuration mode. To reset the access-mode VLAN to the appropriate default VLAN for the device, use the **no** form of this command.

switchport access vlan *vlan-id*
no switchport access vlan

Syntax Description

vlan-id	VLAN to set when the interface is in access mode; valid values are from 1 to 4094. Valid values for Cisco UCS E-Series Servers installed in Cisco 4400 Integrated Services Routers are: • 1-2349—VLAN ID Range 1 • 2450-4095—VLAN ID Range 2

Command Default

The defaults are as follows:

- Access VLAN and trunk-interface native VLAN are default VLANs that correspond to the platform or interface hardware.
- All VLAN lists include all VLANs.

Command Modes

Interface configuration (config-if)

Template configuration (config-template)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 3.9S	This command was implemented on Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Routers (ISR).
Cisco IOS XE Release 3.6E	This command was integrated into Cisco IOS XE Release 3.6E. This command is supported in template configuration mode.

Usage Guidelines

You must enter the **switchport** command without any keywords to configure the LAN interface as a Layer 2 interface before you can enter the **switchport access vlan** command. This action is required only if you have not entered the **switchport** command for the interface.

Entering the **no switchport** command shuts down the port and then reenables it. This action may generate messages on the device to which the port is connected.

The no form of the **switchport access vlan** command resets the access-mode VLAN to the appropriate default VLAN for the device.

Examples

The following example shows how to stop the port interface from operating as a Cisco-routed port and convert to a Layer 2 switched interface:

```
Device(config-if)# switchport
```

Note The **switchport** command is not used on platforms that do not support Cisco-routed ports. All physical ports on such platforms are assumed to be Layer 2-switched interfaces.

The following example shows how to make a port interface that has already been configured as a switched interface to operate in VLAN 2 instead of the platform's default VLAN in interface configuration mode:

```
Device(config-if)# switchport access vlan 2
```

The following example shows how to make a port interface that has already been configured as a switched interface to operate in VLAN 2 instead of the platform's default VLAN, using an interface template in template configuration mode:

```
Device# configure terminal
Device(config)# template user-template1
Device(config-template)# switchport access vlan 2
Device(config-template)# end
```

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
switchport	Configures a LAN interface as a Layer 2 interface.

switchport autostate exclude

To exclude a port from the VLAN interface link-up calculation, use the **switchportautostateexclude**command in interface configuration mode. To return to the default settings, use the **no** form of this command.

switchport autostate exclude
no switchport autostate exclude

Syntax Description

This command has no keywords or arguments.

Command Default

All ports are included in the VLAN interface link-up calculation.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(17b)SXA	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You must enter the **switchport** command without any keywords to configure the LAN interface as a Layer 2 interface before you can enter the **switchportautostateexclude** command. This action is required only if you have not entered the **switchport** command for the interface.

Note The **switchport**command is not used on platforms that do not support Cisco-routed ports. All physical ports on such platforms are assumed to be Layer 2 switched interfaces.

A VLAN interface configured on the MSFC is considered up if there are ports forwarding in the associated VLAN. When all ports on a VLAN are down or blocking, the VLAN interface on the MSFC is considered down. For the VLAN interface to be considered up, all the ports in the VLAN need to be up and forwarding. You can enter the switchport autostate **exclude**command to exclude a port from the VLAN interface link-up calculation.

The switchport autostate **exclude** command marks the port to be excluded from the interface VLAN up calculation when there are multiple ports in the VLAN.

The **showinterface***interface***switchport** command displays the autostate mode if the mode has been set. If the mode has not been set, the autostate mode is not displayed.

Examples

This example shows how to exclude a port from the VLAN interface link-up calculation:

```
Router(config-if)#
switchport autostate exclude
```

This example shows how to include a port in the VLAN interface link-up calculation:

```
Router(config-if)#
no switchport autostate exclude
```

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
switchport	Configures a LAN interface as a Layer 2 interface.

switchport backup

To configure an interface as a Flexlink backup interface, use the **switchport backup** command in interface configuration mode. To disable this configuration, use the **no** form of this command.

switchport backup interface *type number*[{**preemption** {**delay** *delay* | **mode** {**bandwidth** | **forced** | **off**}}}]
no switchport backup [{**interface** *type number* [{**preemption** {**delay** | **mode**}}]}]

Syntax Description

interface *type number*	Specifies the interface type and the module and port number to be configured as a Flexlink backup interface.
preemption delay *delay*	Specifies the preemption delay in seconds. The range is from 0 to 300 seconds.
preemption mode bandwidth	Specifies that a higher bandwidth interface is preferred for preemption.
preemption mode forced	Specifies that an active interface is preferred for preemption.
preemption mode off	Specifies that preemption is turned off.

Command Default

Interfaces are not configured as Flexilink backup interfaces.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)SXF	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.1(1)SY	This command was modified. The **no** form was modified so that specific backup configurations can be disabled.

Usage Guidelines

When you enable Flexlink, both the active and standby links are up physically, and mutual backup is provided.

Flexlink is supported on Layer 2 interfaces only and does not support routed ports.

The *number* arguement designates the module and port number. Valid values depend on the chassis and module that are used. For example, if you have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the slot number are from 1 to 13, and valid values for the port number are from 1 to 48.

Flexlink is designed for simple access topologies (two uplinks from a leaf node). You must ensure that there are no loops from the wiring closet to the distribution/core network to enable Flexlink to perform correctly.

Flexlink converges faster for directly connected link failures. Flexlink fast convergence does not impact any other type of network failure.

You must enter the **switchport** command without any keywords to configure a LAN interface as a Layer 2 interface before you can enter the **switchport backup** command.

You can remove all Flexilink configurations on an interface by using the **no switchport backup** command. You can remove specific backup configurations by using the optional keywords in the **no** form of this command.

Note The **switchport** command is used only on platforms that support Cisco-routed ports. All physical ports on such platforms are assumed to be Layer 2 switched interfaces.

Examples

The following example shows how to enable Flexlink on an interface. This example also shows how to configure a preemption delay of 100 seconds on an interface.

```
Device(config)# interface GigabitEthernet1/1
Device(config-if)# switchport
Device(config-if)# switchport backup interface GigabitEthernet1/2
Device(config-if)# switchport backup interface GigabitEthernet1/2 preemption delay 100
Device(config-if)# end
Device# show running interface GigabitEthernet1/1

Building configuration...

Current configuration : 219 bytes
!
interface GigabitEthernet1/1
 switchport
 switchport backup interface Gi1/2
 switchport backup interface Gi1/2 preemption delay 100
end

Device# show interfaces switchport backup

Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
Gi1/1                   Gi1/2                   Active Up/Backup Down
```

The following example shows how to disable specific backup configurations on an interface:

```
Device(config)# interface GigabitEthernet1/1
Device(config-if)# no switchport backup interface GigabitEthernet1/2 preemption delay
Device(config-if)# end
Device# show running-config interface GigabitEthernet1/1

Building configuration...

Current configuration : 219 bytes
!
interface GigabitEthernet1/1
 switchport
 switchport backup interface Gi1/2
end
```

The following example shows how to disable Flexlink and remove all Flexlink configurations on an interface:

```
Device(config)# interface GigabitEthernet1/1
Device(config-if)# no switchport backup interface GigabitEthernet1/2
Device(config-if)# end
```

```
Device# show running-config interface GigabitEthernet1/1

Building configuration...

Current configuration : 219 bytes
!
interface GigabitEthernet1/1
 switchport
end
```

Related Commands

Command	Description
show interfaces switchport backup	Displays Flexlink pairs.
show running-config	Displays the contents of the current running configuration file or the configuration for a specific module, Layer 2 VLAN, class map, interface, map class, policy map, or VC class.
switchport	Configures a LAN interface as a Layer 2 interface.
switchport autostate exclude	Excludes a port from the VLAN interface link-up calculation.

switchport block unicast

To prevent the unknown unicast packets from being forwarded, use the **switchportblockunicast**command in interface configuration mode. To allow the unknown unicast packets to be forwarded, use the **no** form of this command.

switchport block unicast
no switchport block unicast

Syntax Description

This command has no arguments or keywords.

Command Default

The default settings are as follows:

- Unknown unicast traffic is not blocked.
- All traffic with unknown MAC addresses is sent to all ports.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You can block the unknown unicast traffic on the switch ports.

Blocking the unknown unicast traffic is not automatically enabled on the switch ports; you must explicitly configure it.

Note For more information about blocking the packets, refer to the Cisco 7600 Series Router Cisco IOS Software Configuration Guide.

You can verify your setting by entering the **showinterfaces** *interface-id***switchport** command.

Examples

This example shows how to block the unknown unicast traffic on an interface:

```
Router(config-if)# switchport block unicast
```

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.

switchport capture

To configure the port to capture VACL-filtered traffic, use the **switchportcapture**command in interface configuration mode. To disable the capture mode on the port, use the **no** form of this command.

switchport capture
no switchport capture

Syntax Description

This command has no keywords or arguments.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You must enter the **switchport** command without any keywords to configure the LAN interface as a Layer 2 switched interface before you can enter additional **switchport** commands with keywords. This action is required only if you have not entered the **switchport** command for the interface.

The VACL capture function for the NAM is supported on the Supervisor Engine 720 but is not supported with the IDSM-2.

The **switchportcapture** command applies only to Layer 2 switched interfaces.

WAN interfaces support only the capture functionality of VACLs.

Entering the **noswitchport** command shuts down the port and then reenables it. This action may generate messages on the device to which the port is connected.

Entering the **switchportcapture** command sets the capture function on the interface so that the packets with the capture bit set are received by the interface.

There is no restriction on the order that you enter the **switchportcapture** and **switchportcaptureallowedvlan**commands. The port does not become a capture port until you enter the **switchportcapture** (with no arguments) command.

The capture port must allow the destination VLANs of the captured packets. Once you enable a capture port, the packets are allowed from all VLANs by default, the capture port is on longer in the originally configured mode, and the capture mode enters monitor mode. In monitor mode, the capture port does the following:

- Does not belong to any VLANs that it was in previously.
- Does not allow incoming traffic.
- Preserves the encapsulation on the capture port if you enable the capture port from a trunk port and the trunking encapsulation was ISL or 802.1Q. The captured packets are encapsulated with the corresponding

encapsulation type. If you enable the capture port from an access port, the captured packets are not encapsulated.

- When you enter the **noswitchportcapture** command to disable the capture function, the port returns to the previously configured mode (access or trunk).
- Packets are captured only if the destination VLAN is allowed on the capture port.

Examples

This example shows how to configure an interface to capture VACL-filtered traffic:

```
Router(config-if)# switchport capture
```

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
switchport capture allowed vlan	Specifies the destination VLANs of the VACL-filtered traffic.
switchport	Configures the LAN interface as a Layer 2 switched interface.

switchport capture allowed vlan

To specify the destination VLANs of the VACL-filtered traffic, use the **switchport** capture allowed vlancommand in interface configuration mode. To clear the configured-destination VLAN list and return to the default settings, use the **no** form of this co mmand.

switchport capture allowed vlan {**add** | **all** | **except** | **remove**} *vlanid* [,*vlanid* [,*vlanid*]] [, . . .]
no switchport capture allowed vlan

Syntax Description

add	Adds the specified VLANs to the current list.
all	Adds all VLANs to the current list.
except	Adds all VLANs except the ones that are specified.
remove	Removes the specified VLANs from the current list.
vlan-id	VLAN IDs of the allowed VLANs when this port is in capture mode; valid values are from 1 to 4094.

Command Default

all

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You must enter the **switchport** command without any keywords to configure the LAN interface as a Layer 2-switched interface before you can enter additional **switchport** commands with keywords. This action is required only if you have not entered the **switchport** command for the interface.

The switchport capture allowed vlan command applies only to Layer 2-switched interfaces.

Entering the **noswitchport** command shuts down the port and then reenables it. This action may generate messages on the device to which the port is connected.

You can enter the *vlan-id* as a single VLAN, a group of VLANs, or both. For example, you would enter **switchportcaptureallowedvlan1-1000,2000,3000-3100**.

There is no restriction on the order in which you enter the **switchportcapture** and **switchportcaptureallowedvlan**commands. The port does not become a capture port until you enter the **switchportcapture** (with no arguments) command.

WAN interfaces support only the capture functionality of VACLs.

Examples

This example shows how to add the specified VLAN to capture VACL-filtered traffic:

```
Router(config-if)# switchport capture
 allowed vlan add 100
```

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
switchport	Configures the LAN interface as a Layer 2 switched interface.
switchport capture	Configures the port to capture VACL-filtered traffic.

switchport dot1q ethertype

To specify the EtherType value to be programmed on the interface, use the **switchportdot1qethertype** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

switchport dot1q ethertype *value*
no switchport dot1q ethertype *value*

Syntax Description

value	EtherType value for 802.1Q encapsulation; valid values are from 0x600 to 0xFFFF.

Command Default

The *value* is 0x8100.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(17a)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You can configure a custom EtherType-field value on trunk ports and on access ports.

Each port supports only one EtherType-field value. A port that is configured with a custom EtherType-field value does not recognize frames that have any other EtherType-field value as tagged frames.

Caution A port that is configured with a custom EtherType-field value considers frames that have any other EtherType-field value to be untagged frames. A trunk port that is configured with a custom EtherType-field value puts frames that are tagged with any other EtherType-field value into the native VLAN. An access port or tunnel port that is configured with a custom EtherType-field value puts frames that are tagged with any other EtherType-field value into the access VLAN.

You can configure a custom EtherType-field value on the following modules:

- Supervisor engines
- WS-X6516A-GBIC
- WS-X6516-GBIC

Note The WS-X6516A-GBIC and WS-X6516-GBIC modules apply a configured custom EtherType-field value to all ports that are supported by each port ASIC (1 through 8 and 9 through 16).

- WS-X6516-GE-TX
- WS-X6748-GE-TX

- WS-X6724-SFP
- WS-X6704-10GE
- WS-X6816-GBIC

You cannot configure a custom EtherType-field value on the ports in an EtherChannel.

You cannot form an EtherChannel from ports that are configured with custom EtherType-field values.

Examples

This example shows how to set the EtherType value to be programmed on the interface:

```
Router (config-if)# switchport dot1q ethertype 1234
```

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.

switchport mode

To set the interface type, use the **switchport mode** command in interface configuration mode. Use the appropriate **no** form of this command to reset the mode to the appropriate default mode for the device.

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers
switchport mode {**access** | **trunk**}
no switchport mode

Cisco Catalyst 6500/6000 Series Switches
switchport mode {**access** | **dot1q-tunnel** | **dynamic** {**auto** | **desirable**} | **trunk**}
no switchport mode

Cisco 7600 Series Routers
switchport mode {**access** | **dot1q-tunnel** | **dynamic** {**auto** | **desirable**} | **private-vlan** | **trunk**}
no switchport mode
switchport mode private-vlan {**host** | **promiscuous**}
no switchport mode private-vlan

Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers
switchport mode {**access** | **trunk**}
no switchport mode {**access** | **trunk**}

Syntax Description

access	Sets a nontrunking, nontagged single VLAN Layer 2 interface.
trunk	Specifies a trunking VLAN Layer 2 interface.
dot1q-tunnel	Sets the trunking mode to TUNNEL unconditionally.
dynamic auto	Sets the interface to convert the link to a trunk link.
dynamic desirable	Sets the interface to actively attempt to convert the link to a trunk link.
private vlan host	Specifies that the ports with a valid private VLAN (PVLAN) association become active host private VLAN ports.
private vlan promiscuous	Specifies that the ports with a valid PVLAN mapping become active promiscuous ports.

Table 282: Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers

access	Sets a nontrunking, nontagged single VLAN Layer 2 interface.
trunk	Specifies a trunking VLAN Layer 2 interface.

Command Default

The default is **access** mode.

The default mode is dependent on the platform; it should be either **dynamic auto** for platforms that are intended as wiring closets or **dynamic desirable** for platforms that are intended as backbone switches. The default for PVLAN ports is that no mode is set.

The defaults are as follows:

- The mode is dependent on the platform; it should either be **dynamic auto** for platforms that are intended for wiring closets or **dynamic desirable** for platforms that are intended as backbone switches.
- No mode is set for PVLAN ports.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(7)XE	This command was introduced on the Cisco Catalyst 6000 family switches.
12.1(1)E	This command was integrated on the Cisco Catalyst 6000 family switches.
12.1(8a)EX	The switchport mode **private-vlan** {**host** | **promiscuous**} syntax was added.
12.2(2)XT	Creation of switchports became available on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T for creation of switchports on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
Cisco IOS XE Release 3.9S	This command was implemented on Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Routers (ISR).

Usage Guidelines

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

If you enter a forced mode, the interface does not negotiate the link to the neighboring interface. Ensure that the interface ends match.

The **no** form of the command is not supported on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Cisco Catalyst 6500/6000 Switches and Cisco 7600 Series Routers

If you enter **access** mode, the interface goes into permanent nontrunking mode and negotiates to convert the link into a nontrunk link even if the neighboring interface does not agree to the change.

If you enter **trunk** mode, the interface goes into permanent trunking mode and negotiates to convert the link into a trunk link even if the neighboring interface does not agree to the change.

If you enter **dynamic auto** mode, the interface converts the link to a trunk link if the neighboring interface is set to **trunk** or **desirable** mode.

If you enter **dynamic desirable** mode, the interface becomes a trunk interface if the neighboring interface is set to **trunk**, **desirable**, or **auto** mode.

If you configure a port as a promiscuous or host-PVLAN port and one of the following applies, the port becomes inactive:

- The port does not have a valid PVLAN association or mapping configured.
- The port is a SPAN destination.

If you delete a private-port PVLAN association or mapping, or if you configure a private port as a SPAN destination, the deleted private-port PVLAN association or mapping or the private port that is configured as a SPAN destination becomes inactive.

If you enter **dot1q-tunnel** mode, PortFast Bridge Protocol Data Unit (BPDU) filtering is enabled and Cisco Discovery Protocol (CDP) is disabled on protocol-tunneled interfaces.

Examples

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

The following example shows how to set the interface to **access** mode:

```
Router#configure terminal
Router(config)# interface fastethernet 4/1
Router(config-if)#switchport mode access
```

The following example shows how to set the interface to **trunk** mode:

```
Router#configure terminal
Router(config)# interface fastethernet 4/1
Router(config-if)#switchport mode trunk
```

Cisco Catalyst 6500/6000 Switches and Cisco 7600 Series Routers

The following example shows how to set the interface to dynamic desirable mode:

```
Router#configure terminal
Router(config)# interface fastethernet 4/1
Router(config-if)# switchport mode dynamic desirable
```

The following example shows how to set a port to PVLAN-host mode:

```
Router#configure terminal
Router(config)# interface fastethernet 4/1
Router(config-if)# switchport mode private-vlan host
```

The following example shows how to set a port to PVLAN-promiscuous mode:

```
Router#configure terminal
Router(config)# interface fastethernet 4/1
Router(config-if)# switchport mode private-vlan promiscuous
```

Integrated Series Routers Generation 2 (ISR G2) Platforms with EHWIC-4/8ESG

The following example shows how to configure tunneling on port 4/1 and verify the configuration:

```
Router#configure terminal
Router(config)# interface fastethernet 4/1
Router(config-if)# switchport mode dot1q-tunnel
Router(config-if)# end
```

Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers

The following example shows how to set the interface to **access** mode:

```
Router#configure terminal
Router(config)# interface ucse 1/0/0
Router(config-if)# switchport mode access
```

The following example shows how to set the interface to **trunk** mode:

```
Router#configure terminal
Router(config)# interface ucse 1/0/0
Router(config-if)# switchport mode trunk
```

Related Commands

Command	Description
show dot1q-tunnel	Displays a list of 802.1Q tunnel-enabled ports.
show interfaces switchport	Displays administrative and operational status of a switching (nonrouting) port.
show interfaces trunk	Displays trunk information.
switchport	Modifies the switching characteristics of the Layer 2-switched interface.
switchport private vlan host association	Defines a PVLAN association for an isolated or community port.
switchport private vlan mapping	Defines the PVLAN mapping for a promiscuous port.
switchport trunk	Sets trunk characteristics when the interface is in trunking mode.

switchport port-security

To enable port security on an interface, use the **switchportport-security** command in i nterface configuration mode . To disable port security, use the **no** form of this command.

switchport port-security
no switchport port-security

Syntax Description

This command has no keywords or arguments.

Command Default

D isabled

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXE	This command was changed as follows on the Supervisor Engine 720: • With Release 12.2(18)SXE and later releases, port security is supported on trunks. • With Release 12.2(18)SXE and later releases, port security is supported on 802.1Q tunnel ports.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Follow these guidelines when configuring port security:

- With Release 12.2(18)SXE and later releases, port security is supported on trunks.
- With releases earlier than Release 12.2(18)SXE, port security is not supported on trunks.
- With Release 12.2(18)SXE and later releases, port security is supported on 802.1Q tunnel ports.
- With releases earlier than Release 12.2(18)SXE, port security is not supported on 802.1Q tunnel ports.
- A secure port cannot be a destination port for a Switch Port Analyzer (SPAN).
- A secure port cannot belong to an EtherChannel.
- A secure port cannot be a trunk port.
- A secure port cannot be an 802.1X port. If you try to enable 802.1X on a secure port, an error message appears, and 802.1X is not enabled. If you try to change an 802.1X-enabled port to a secure port, an error message appears, and the security settings are not changed.

Examples

This example shows how to enable port security:

```
Router(config-if)#
switchport port-security
```

This example shows how to disable port security:

Related Commands

Command	Description
show port-security	Displays information about the port-security setting.

switchport port-security aging

To configure the port security aging , use the **switchport** port-security aging time command in interface configuration mode . To disable aging, use the **no** form of this command.

switchport port-security aging {**time** *time* | **type** {**absolute** | **inactivity**}}
no switchport port-security aging

Syntax Description

time *time*	Sets the duration for which all addresses are secured; valid values are from 1 to 1440 minutes.
type	Specifies the type of aging.
absolute	Specifies absolute aging; see the "Usage Guidelines" section for more information.
inactivity	Specifies that the timer starts to run only when there is no traffic; see the "Usage Guidelines" section for more information.

Command Default

The defaults are as follows:

- Disabled.
- If enabled, t he defaults are as follows:
  - *time* is 0.
  - **type** is **absolute**

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXE	This command was changed as follows on the Supervisor Engine 720: • With Release 12.2(18)SXE and later releases, port security is supported on trunks. • With Release 12.2(18)SXE and later releases, port security is supported on 802.1Q tunnel ports. • The **type**, **absolute**, and **inactivity** keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Follow these guidelines when configuring port security:

- With Release 12.2(18)SXE and later releases, port security is supported on trunks. With releases earlier than Release 12.2(18)SXE, port security is not supported on trunks.
- With Release 12.2(18)SXE and later releases, port security is supported on 802.1Q tunnel ports. With releases earlier than Release 12.2(18)SXE, port security is not supported on 802.1Q tunnel ports.

You can apply one of two types of aging for automatically learned addresses on a secure port:

- Absolute aging times out the MAC address after the age-time has been exceeded, regardless of the traffic pattern. This default is for any secured port, and the age-time is set to 0.
- Inactivity aging times out the MAC address only after the age_time of inactivity from the corresponding host has been exceeded.

Examples

This example shows how to set the aging time as 2 hours:

```
Router(config-if)# switchport port-security aging time 120
```

This example shows how to set the aging time as 2 minutes:

```
Router(config-if)# switchport port-security aging time 2
```

This example shows how to set the aging type on a port to absolute aging:

```
Router(config-if) switchport port-security aging type absolute
```

This example shows how to set the aging type on a port to inactivity aging:

```
Router(config-if) switchport port-security aging type
 inactivity
```

Related Commands

Command	Description
show port-security	Displays information about the port-security setting.

switchport port-security mac-address

To add a MAC address to the list of secure MAC addresses, use the **switchportport-securitymac-address** command. To remove a MAC address from the list of secure MAC addresses, use the **no** form of this command.

switchport port-security mac-address {*mac-addr* | **sticky** [*mac-addr*] [{**vlan** *vlan* [**voice**]*vlan-list*}]}
no switchport port-security mac-address {*mac-addr* | **sticky** [*mac-addr*] [{**vlan** *vlan* [**voice**]*vlan-list*}]}

Syntax Description

mac-addr	MAC addresses for the interface; valid values are from 1 to 1024.
sticky	Configures the dynamic MAC addresses as sticky on an interface.
vlan *vlan* | *vlan-list*	(Optional) Specifies a VLAN or range of VLANs; see the "Usage Guidelines" section for additional information.

Command Default

MAC-addresses are not classified as secured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXE	This command was changed as follows on the Supervisor Engine 720: • With Release 12.2(18)SXE and later releases, port security is supported on trunks. • With Release 12.2(18)SXE and later releases, port security is supported on 802.1Q tunnel ports. • The **vlan***vlan* | *vlan-list*keyword and arguments were added. • The **sticky** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If you configure fewer secure MAC addresses than the maximum number of secure MAC addresses on all interfaces, the remaining MAC addresses are dynamically learned.

To clear multiple MAC addresses, you must enter the **no** form of this command once for each MAC address to be cleared.

The *vlan-list* argument is visible only if the port has been configured and is operational as a trunk. Enter the **switchportmodetrunk** command and then enter the **switchportnonegotiate** command.

The **sticky** keyword configures the dynamic MAC addresses as sticky on an interface. Sticky MAC addresses configure the static Layer 2 entry to stay sticky to a particular interface. This feature can prevent MAC moves or prevent the entry from being learned on a different interface.

You can configure the sticky feature even when the port security feature is not enabled on the interface. It becomes operational once port security is enabled on the interface.

Note You can enter the **switchportport-securitymac-addresssticky** command only if sticky is enabled on the interface.

When port security is enabled, disabling the sticky feature causes all configured and learned sticky addresses to be deleted from the configuration and converted into dynamic secure addresses.

When port security is disabled, disabling the sticky feature causes all configured and learned sticky addresses to be deleted from the configuration.

For trunk ports, if you enter the **noswitchportport-securitymac-addresssticky** command, a search is conducted for the MAC address in the native VLAN. An error message is displayed if the MAC address is not found in the native VLAN. You must specify the VLAN in the **no** form of the **switchportport-securitymac-addresssticky** command to remove the MAC address.

For voice ports, you must specify the **vlanvoice** keywords in the **no** form of the command.

Examples

This example shows how to configure a secure MAC address:

```
Router(config-if)# switchport port-security mac-address 1000.2000.3000
```

This example shows how to delete a secure MAC address from the address table:

```
Router(config-if)# no switchport port-security mac-address 1000.2000.3000
```

This example shows how to enable the sticky feature on an interface:

```
Router(config-if)# switchport port-security mac-address sticky
```

This example shows how to disable the sticky feature on an interface:

```
Router(config-if)# no switchport port-security mac-address sticky
```

This example shows how to make a specific MAC address as a sticky address:

```
Router(config-if)# switchport port-security mac-address sticky 0000.0000.0001
```

This example shows how to delete a specific sticky address:

```
Router(config-if)# no switchport port-security mac-address sticky 0000.0000.0001
```

This example shows how to delete all sticky and static addresses that are configured on an interface:

```
Router(config-if)# no switchport port-security mac-address
```

The following example shows how to configure a VLAN in the voice port:

```
Router(config-if)# switch port-security mac-address 0.0.1 vlan voice
```

To remove the MAC address 0.0.1 from the voice port, use the following command:

```
Router(config-if)# no switchport port-security mac-address 0.0.1 vlan voice
```

Related Commands

Command	Description
clear port-security	Deletes configured secure MAC addresses and sticky MAC addresses from the MAC address table.
show port-security	Displays information about the port-security setting.
switchport mode trunk	Configures the port as a trunk member.
switchport nonegotiate	Configures the LAN port into permanent trunking mode.

switchport port-security maximum

To set the maximum number of secure MAC addresses on a port, use the **switchportport-securitymaximum**command in interface configuration mode. To return to the default settings, use the **no** form of this command.

switchport port-security maximum *maximum* [{**vlan** *vlanvlan-list*}]
no switchport port-security maximum

Syntax Description

maximum	M aximum number of secure MAC addresses for the interface; valid values are from 1 to 4097.
vlan *vlan* | *vlan-list*	(Optional) Specifies a VLAN or range of VLANs; see the "Usage Guidelines" section for additional information.

Command Default

This command has no default setings .

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the Release 12.2(17d)SXB.
12.2(18)SXE	This command was changed as follows on the Supervisor Engine 720 only: • The maximum number of secure MAC addresses was changed from 1024 to 4097. • The **vlan***vlan* | *vlan-list*keyword and arguments were added. • With Release 12.2(18)SXE and later releases, port security is supported on trunks. • With Release 12.2(18)SXE and later releases, port security is supported on 802.1Q tunnel ports.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If you enter this command more than once, subsequent use of this command overrides the previous value of *maximum*. If the new *maximum*argument is larger than the current number of the secured addresses on this port, there is no effect except to increase the value of the *maximum*.

If the new *maximum* is smaller than the old *maximum* and there are more secure addresses on the old *maximum*, the command is rejected.

If you configure fewer secure MAC addresses than the maximum number of secure MAC addresses on the port, the remaining MAC addresses are dynamically learned.

Once the maximum number of secure MAC addresses for the port is reached, no more addresses are learned on that port even if the per-VLAN port maximum is different from the aggregate maximum number.

You can override the maximum number of secure MAC addresses for the port for a specific VLAN or VLANs by entering the **switchportport-securitymaximum***maximum***vlan***vlan*|*vlan-list*command.

The *vlan-list* argument allows you to enter ranges, commas, and delimited entries such as 1,7,9-15,17.

The *vlan-list* argument is visible only if the port has been configured and is operational as a trunk. Enter the **switchportmodetrunk** command and then enter the **switchportnonegotiate** command.

Examples

This example shows how to set the maximum number of secure MAC addresses that are allowed on this port:

```
Router(config-if)# switchport port-security maximum 5
```

This command shows how to override the maximum set for a specific VLAN:

```
Router(config-if)# switchport port-security maximum 3 vlan 102
```

Related Commands

Command	Description
show port-security	Display information about the port-security setting.
switchport nonegotiate	Configures the LAN port into permanent trunking mode.

switchport port-security violation

To set the action to be taken when a security violation is detected, use the **switchportport-securityviolation** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

switchport port-security violation {**shutdown** | **restrict** | **protect**}
no switchport port-security violation {**shutdown** | **restrict** | **protect**}

Syntax Description

shutdown	Shuts down the port if there is a security violation.
restrict	Drops all the packets from the insecure hosts at the port-security process level and increments the security-violation count.
protect	Drops all the packets from the insecure hosts at the port-security process level but does not increment the security-violation count.

Command Default

The port security violation is shutdown.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXE	This command was changed as follows on the Supervisor Engine 720: • With Release 12.2(18)SXE and later releases, port security is supported on trunks. • With Release 12.2(18)SXE and later releases, port security is supported on 802.1Q tunnel ports.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(14)SXH	**Platform port-security disable traps** was introduced as part of protect violation mode.

Usage Guidelines

When a security violation is detected, one of the following actions occurs:

- Protect--When the number of port-secure MAC addresses reaches the maximum limit that is allowed on the port, the packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses. Platform port-security disable traps is configurable only when the violation mode is set to **protect**. When this option is configured, drop entries will not be installed into hardware for violating addresses, thus allowing traffic to continue to flow to violating address from legitimate ports. To protect switch CPU against overload when this option is enabled, we recommend that you configure the port-security rate-limiter to 2000 packets per second with a burst rate of 10.

Note This feature also permits traffic to legitimate ports from insecure MAC addresses.

- Restrict--A port-security violation restricts data and causes the security-violation counter to increment.
- Shutdown--The interface is error disabled when a security violation occurs.

Note When a secure port is in the error-disabled state, you can bring it out of this state by entering the **errdisablerecoverycausepsecure-violation** global configuration command or you can manually reenable it by entering the **shutdown** and **noshutdown** commands in interface-configuration mode.

Examples

This example shows how to set the action to be taken when a security violation is detected:

```
Router(config-if)# switchport port-security violation restrict
```

This example allows the traffic to a secured MAC address on one port to flow even in the presence of violations on other ports while in protect mode.

```
Router(config-if)# switchport port-security violation protect
Router(config-if)# platform port-security disable traps
```

Related Commands

Command	Description
show port-security	Displays information about the port-security setting.
errdisable recovery cause psecure-violation (global configuration)	Removes a secure port from an error-disabled state.
platform port-security disable traps	Modifies the behavior of protect violation mode.

switchport private-vlan host-association

To define a PVLAN association for an isolated or community port, use the **switchportprivate-vlanhost-association**command in i nterface configuration mode . To remove the PVLAN mapping from the port, use the **no** form of this command.

switchport private-vlan host-association *primary-vlan-id secondary-vlan-id*
no switchport private-vlan host-association

Syntax Description

primary-vlan-id	Number of the primary VLAN of the PVLAN relationship; valid values are from 1 to 4094.
secondary-vlan-id	Number of the secondary VLAN of the private VLAN relationship; valid values are from 1 to 4094.

Command Default

No PVLAN is configured.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to t Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

There is no run-time effect on the port unless it is in PVLAN-host mode. If the port is in PVLAN-host mode but neither of the VLANs exist, the command is allowed but the port is made inactive.

The secondary VLAN may be an isolated or community VLAN.

Examples

This example shows how to configure a port with a primary VLAN (VLAN 18) and secondary VLAN (VLAN 20):

```
Router(config-if)#
switchport private-vlan host-association 18 20
```

This example shows how to remove the PVLAN association from the port:

```
Router(config-if)#
no switchport private-vlan host-association
```

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.

Command	Description
switchport mode	Displays the administrative and operational status of a switching (nonrouting) port.

switchport private-vlan mapping

To define the PVLAN mapping for a promiscuous port, use the **switchportprivate-vlanmapping** command in interface configuration mode. To clear all mappings from the primary VLAN, use the **no** form of this command.

{**switchport private-vlan mapping primary-vlan-id secondary-vlan-list | add secondary-vlan-list | remove secondary-vlan-list**}
no switchport private-vlan mapping

Syntax Description

primary-vlan-id	Number of the primary VLAN of the PVLAN relationship; valid values are from 1 to 4094.
secondary-vlan- list	Number of the secondary VLAN of the private VLAN relationship; valid values are from 1 to 4094.
add	Maps the secondary VLANs to the primary VLAN.
remove	Clears mapping between the secondary VLANs and the primary VLAN.

Command Default

No PVLAN mappings are configured.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

There is no run-time effect on the port unless it is in PVLAN-promiscuous mode. If the port is in PVLAN-promiscuous mode but the VLANs do not exist, the command is allowed but the port is made inactive.

The secondary VLAN may be an isolated or community VLAN.

Examples

This example shows how to configure the mapping of primary VLAN 18 to secondary isolated VLAN 20 on a port:

```
Router(config-if)#
switchport private-vlan mapping 18 20
```

This example shows how to add a VLAN to the mapping:

```
Router(config-if)#
switchport private-vlan mapping 18 add 21
```

This example shows how to remove the PVLAN mapping from the port:

```
Router(config-if)#
no switchport private-vlan mapping
```

Related Commands

Command	Description
show interfaces private-vlan mapping	Displays the information about the PVLAN mapping for VLAN SVIs.

switchport protected

Use the switch**portprotected**command to isolate unicast, multicast, and broadcast traffic at Layer 2 from other protected ports on the same switch in interface configuration mode. To disable protection on the port, use the **no** form of the command.

switchport protected
no switchport protected

Syntax Description

This command has no arguments or keywords.

Command Default

No protected port is defined. All ports are nonprotected.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1(4)EA1	This command was first introduced.
12.4(15)T	This command was implemented on the following platforms: the Cisco 1841 Integrated Services Router (ISR), Cisco 2800 series ISRs, and Cisco 3800 series ISRs.

Usage Guidelines

The switchport protection feature is local to the switch; communication between protected ports on the same switch is possible only through a Layer 3 device. To prevent communication between protected ports on different switches, you must configure the protected ports for unique VLANs on each switch and configure a trunk link between the switches.

Beginning with Cisco IOS Release 12.4(15)T, the following Cisco ISRs support port protection when an appropriate high-speed WAN interface card (HWIC) is installed:

- Cisco 1841 ISR
- Cisco 2800 Series ISRs, including models 2801, 2811, 2821, and 2851
- Cisco 3800 Series ISRs, including models 3825 and 3845

To support port protection, the Cisco routers listed above must be equipped with one of the following HWICs:

- HWIC-4ESW
- HWIC-D-9ESW

Note Only the ports attached to the HWICs can be configured with port protection.

A protected port does not forward any unicast, multicast, or broadcast traffic to any other protected port. A protected port continues to forward unicast, multicast, and broadcast traffic to unprotected ports and vice versa.

Port monitoring does not work if both the monitor and monitored ports are protected ports.

A protected port is different from a secure port.

Examples

The following example shows how to enable a protected port on an interface:

```
Switch(config)# interface gigabitethernet0/3
Switch(config-if)# switchport protected
```

You can verify the previous command by entering the**showinterfacesswitchport**privileged EXEC command.

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
switchport block	Prevents unknown multicast or unicast traffic on the interface.

switchport trunk

To set the trunk characteristics when the interface is in trunking mode, use the **switchport trunk** command in interface configuration mode. To reset all of the trunking characteristics back to the original defaults, use the **no** form of this command.

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers
switchport trunk {**encapsulation dot1q** | **native vlan** | **allowed vlan**}
no switchport trunk {**encapsulation dot1q** | **native vlan** | **allowed vlan**}

Cisco 7600 Series Routers and Catalyst 6500 Series Switches
{**switchport trunk encapsulation** {**isl** | **dot1q** [**ethertype** *value*] | **negotiate**} | **native vlan** {**tag***vlan-id*} | **allowed vlan** *vlan-list* | **pruning vlan** *vlan-list*}
no switchport trunk {**encapsulation** {**isl** | **dot1q** [**ethertype** *value*] | **negotiate**} | **native vlan** [**tag**] | **allowed vlan** | **pruning vlan**}

Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers
switchport trunk {**native vlan** *vlan-id* | **allowed vlan** *vlan-list*}
no switchport trunk {**native vlan** *vlan-id* | **allowed vlan** *vlan-list*}

Syntax Description

encapsulation isl	Sets the trunk encapsulation format to Inter-Switch Link (ISL).
encapsulation dot1q	Sets the trunk encapsulation format to 802.1Q.
native vlan	Sets the native VLAN for the trunk in 802.1Q trunking mode.
allowed vlan *vlan list*	Sets the list of allowed VLANs that transmit traffic from this interface in tagged format when in trunking mode.
ethertype *value*	(Optional) Sets the EtherType value; valid values are from 0x0 to 0x5EF-0xFFFF.
encapsulation negotiate	Specifies that if the Dynamic Inter-Switch Link (DISL) protocol and Dynamic Trunking Protocol (DTP) negotiation do not resolve the encapsulation format, ISL is the selected format.
native vlan tag	Enables the native VLAN tagging state on the interface.
native vlan *vlan id*	The particular native VLAN.
pruning vlan *vlan list*	Sets the list of VLANs that are enabled for VLAN Trunking Protocol (VTP) pruning when the interface is in trunking mode. See the “Usage Guidelines” section for the *vlanlist*argument formatting guidelines.

Table 283: Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers

native vlan *vlan-id*	The particular native VLAN. Valid values are: • 1-2349—VLAN ID Range 1 • 2450-4095—VLAN ID Range 2

allowed vlan *vlan-list*	Sets the list of allowed VLANs that transmit traffic from this interface in tagged format when in trunking mode. **Note** For *vlan-list* format, see **Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers** section under **Usage Guidelines**.

Command Default

- The default encapsulation type is dot1q.
- The default access VLAN and trunk interface native VLAN are default VLANs that correspond to the platform or interface hardware.
- The default for all VLAN lists is to include all VLANs.

- The encapsulation type is dependent on the platform or interface hardware.
- The access VLAN and trunk interface native VLAN are default VLANs that correspond to the platform or interface hardware.
- The default for all VLAN lists is to include all VLANs.
- **ethertype** *value* for 802.1Q encapsulation is 0x8100.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(7)XE	This command was introduced on the Catalyst 6500 series switches.
12.1(1)E	Switchport creation on Catalyst 6500 series switches was added.
12.2(2)XT	This command was introduced to support switchport creation on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T to support switch port creation on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX to support the Supervisor Engine 720 on the Cisco 7600 series routers and Catalyst 6500 series switches.
12.2(17a)SX	This command was modified to include the following: • Restriction of ISL trunk-encapsulation. • Addition of the **dot1q** keyword and **ethertype***value* keyword and argument.
12.2(17d)SXB	Support for the Supervisor Engine 2 on the Cisco 7600 series routers and Catalyst 6500 series switches was added.
12.2(18)SXD	This command was modified to allow the **switchport trunk allowed vlan**command to be entered on interfaces where the span destination port is either a trunk or an access port.

Release	Modification
12.2(18)SXE	This command added a restriction that Gigabit Ethernet (GE) Optimized Layer 2 WAN ports are not supported on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(15)T	This command was modified to extend the range of valid VLAN IDs from 1 to 4094 for specified platforms.
12.2(33)SXH	This command was changed as follows: • Allowed the tagging of native VLAN traffic on a per-port basis. • Introduced on the Supervisor Engine 720-10GE.
Cisco IOS XE Release 3.9S	This command was implemented on Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Routers (ISR).

Usage Guidelines

802.1Q Trunks

- When you connect Cisco switches through an 802.1Q trunk, make sure that the native VLAN for an 802.1Q trunk is the same on both ends of the trunk link. If the native VLAN on one end of the trunk is different from the native VLAN on the other end, spanning-tree loops might result.
- Disabling spanning tree on the native VLAN of an 802.1Q trunk without disabling spanning tree on every VLAN in the network can cause spanning-tree loops. Cisco recommends that you leave spanning tree enabled on the native VLAN of an 802.1Q trunk. If this is not possible, disable spanning tree on every VLAN in the network. Make sure that your network is free of physical loops before disabling spanning tree.
- When you connect two Cisco switches through 802.1Q trunks, the switches exchange spanning-tree bridge protocol data units (BPDUs) on each VLAN allowed on the trunks. The BPDUs on the native VLAN of the trunk are sent untagged to the reserved IEEE 802.1d spanning-tree multicast MAC address (01-80-C2-00-00-00). The BPDUs on all other VLANs on the trunk are sent tagged to the reserved Shared Spanning Tree Protocol (SSTP) multicast MAC address (01-00-0c-cc-cc-cd).
- The 802.1Q switches that are not Cisco switches maintain only a single instance of spanning-tree (Mono Spanning Tree [MST]) that defines the spanning-tree topology for all VLANs. When you connect a Cisco switch to a switch through an 802.1Q trunk without a Cisco switch, the MST of the switch and the native VLAN spanning tree of the Cisco switch combine to form a single spanning-tree topology known as the Common Spanning Tree (CST).
- Because Cisco switches transmit BPDUs to the SSTP multicast MAC address on VLANs other than the native VLAN of the trunk, switches that are not Cisco switches do not recognize these frames as BPDUs and flood them on all ports in the corresponding VLAN. Other Cisco switches connected to the 802.1Q cloud receive these flooded BPDUs. This condition allows Cisco switches to maintain a per-VLAN spanning-tree topology across a cloud of 802.1Q switches that are not Cisco switches. The 802.1Q cloud of switches separating the Cisco switches is treated as a single broadcast segment among all switches connected to the 802.1Q cloud of switches that are not Cisco switches through 802.1Q trunks.
- Make sure that the native VLAN is the same on *all* of the 802.1Q trunks that connect the Cisco switches to the 802.1Q cloud of switches that are not Cisco switches.

- If you are connecting multiple Cisco switches to a 802.1Q cloud of switches that are not Cisco switches, all of the connections must be through 802.1Q trunks. You cannot connect Cisco switches to an 802.1Q cloud of switches that are not Cisco switches through ISL trunks or through access ports. Doing so will cause the switch to place the ISL trunk port or access port into the spanning-tree “port inconsistent” state and no traffic will pass through the port.

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

The **switchport trunk encapsulation** command is supported only for platforms and interface hardware that can support 802.1Q formats.

The *vlanlist* format is **all | none | add | remove | except***vlanlist*[,*vlanlist*...] where:

- **all** --Specifies all VLANs from 1 to 1005. Beginning with Cisco IOS Release 12.4(15)T, the valid VLAN ID range is from 1 to 4094.
- **none** --Indicates an empty list. This keyword is not supported in the **switchport trunk allowed vlan** form of the command.
- **add** --Adds the defined list of VLANs to those currently set instead of replacing the list.
- **remove** --Removes the defined list of VLANs from those currently set instead of replacing the list.
- **except** --Lists the VLANs that should be calculated by inverting the defined list of VLANs.
- *vlan list*-- Is either a single VLAN number from 1 to 1005 or a continuous range of VLANs described by two VLAN numbers, the lesser one first, separated by a hyphen that represents the VLAN IDs of the allowed VLANs when this port is in trunking mode. Beginning with Cisco IOS Release 12.4(15)T, the valid VLAN ID range is from 1 to 4094.

Cisco 7600 Series Routers and Catalyst 6500 Series Switches

This command is not supported on GE Layer 2 WAN ports.

You can enter the **switchport trunk** command only on the PO. If you enter the **switchport trunk** command on a port member the following message is displayed:

```
Configuration is not allowed on Port members. Remove the interface from the Port Channel
to modify its config
```

The **switchport trunk encapsulation dot1q**command is supported only for platforms and interface hardware that can support both ISL and 802.1Q formats. Only 802.1Q encapsulation is supported by shared port adapters (SPAs).

If you enter the **switchport trunk encapsulation isl** command on a port channel containing an interface that does not support ISL-trunk encapsulation, the command is rejected.

You can enter the **switchport trunk allowed vlan** command on interfaces where the span destination port is either a trunk or an access port.

You can enter the **switchport trunk native vlan tag** command to enable the tagging of native VLAN traffic on a per-port basis. When tagging is enabled, all the packets on the native VLAN are tagged and all incoming untagged data packets are dropped, but untagged control packets are accepted. When tagging is disabled, the native VLAN packets going out on trunk ports are not tagged and the incoming untagged packets are allowed and assigned to the native VLAN. The **no switchport trunknative vlan tag** command overrides the **vlan dot1q tag native** command for global tagging.

Note The **switchport trunk native vlan tag** interface configuration mode command does not enable native VLAN tagging unless you first configure the switch to tag native VLAN traffic globally. To enable native VLAN tagging globally, use the **vlan dot1q tag native** command in global configuration mode.

Note The **switchport trunk pruning vlan** *vlan-list* command does not support extended-range VLANs; valid *vlan-list* values are from 1 to 1005.

The **dot1q ethertype** *value* keyword and argument are not supported on port-channel interfaces. You can enter the command on the individual port interface only. Also, you can configure the ports in a channel group to have different EtherType configurations.

Caution Be careful when configuring the custom EtherType value on a port. If you enter the **negotiate** keyword and DISL and Dynamic Trunking Protocol (DTP) negotiation do not resolve the encapsulation format, then ISL is the selected format and may pose as a security risk. The **no** form of this command resets the trunk-encapsulation format to the default.

- The **no** form of the **switchport trunk native vlan** command resets the native mode VLAN to the appropriate default VLAN for the device.
- The **no** form of the **switchport trunk native vlan tag** command configures the Layer 2 port not to tag native VLAN traffic.
- The **no** form of the **switchport trunk allowed vlan** command resets the list to the default list, which allows all VLANs.
- The **no** form of the **switchport trunk pruning vlan**command resets the list to the default list, which enables all VLANs for VTP pruning.
- The **no** form of the **switchport trunk encapsulation dot1qethertype***value* command resets the list to the default value.

The *vlan-list* format is **all** | **none** | **add** | **remove** | **except** [*vlan-list*[**,***vlan-list*...]] where:

- **all** --Specifies all the appropriate VLANs. This keyword is not supported in the **switchporttrunkpruningvlan** command.
- **none** --Indicates an empty list. This keyword is not supported in the **switchporttrunkallowedvlan** command.
- **add** *vlan-list* **,** *vlan-list...*]-- Adds the defined list of VLANs to those currently set instead of replacing the list.
- **remove** *vlan-list* **,** *vlan-list...*]-- Removes the defined list of VLANs from those currently set instead of replacing the list. You can remove VLAN 1. If you remove VLAN 1 from a trunk, the trunk interface continues to send and receive management traffic (for example, Cisco Discovery Protocol, version 3; VTP; Port Aggregation Protocol, version 4 (PAgP4); and DTP) in VLAN 1.

Note You can remove any of the default VLANs (1002 to 1005) from a trunk; this action is not allowed in earlier releases.

- **except** *vlan-list* **,** *vlan-list...*] --Excludes the specified list of VLANs from those currently set instead of replacing the list.
- *vlan-list* **,** *vlan-list...* -- Specifies a single VLAN number from 1 to 4094 or a continuous range of VLANs that are described by two VLAN numbers from 1 to 4094. You can specify multiple VLAN numbers or ranges of numbers using a comma-separated list.

To specify a range of VLANs, enter the smaller VLAN number first, separated by a hyphen and the larger VLAN number at the end of the range.

Do not enable the reserved VLAN range (1006 to 1024) on trunks when connecting a Cisco 7600 series router running the Cisco IOS software on both the supervisor engine and the Multilayer Switch Feature Card (MSFC) to a Cisco 7600 series router running the Catalyst operating system. These VLANs are reserved in Cisco 7600 series routers running the Catalyst operating system. If enabled, Cisco 7600 series routers running the Catalyst operating system may disable the ports if a trunking channel is between these systems.

Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers

Note To set trunk characteristics, the interface must be in trunk mode.

The *vlan-list* format is **all** | **none** | **add** | **remove** | **except** | **WORD**, where:

- **all**—Specifies all VLANs: 1-2349—VLAN IDs in range 1; and 2450-4095—VLAN IDs in range 2.
- **none**—Indicates an empty list.
- **add**—Adds the defined list of VLANs to those currently set instead of replacing the list.
- **remove**—Removes the defined list of VLANs from those currently set instead of replacing the list.
- **except**—Lists the VLANs that should be calculated by inverting the defined list of VLANs.
- **WORD**—Is either a single VLAN number from 1 to 4095 or a continuous range of VLANs described by two VLAN numbers, the lesser one first, separated by a hyphen that represents the VLAN IDs of the allowed VLANs when this port is in trunking mode.

Examples

The following example shows how to cause a port interface configured as a switched interface to encapsulate in 802.1Q trunking format regardless of its default trunking format in trunking mode:

Router(config-if)# switchport trunk encapsulation dot1q

The following example shows how to configure the Layer 2 port to tag native VLAN traffic:

```
Router(config-if)#
switchport trunk native vlan tag
```

Cisco UCS E-Series Server Installed in Cisco 4400 Integrated Services Routers

Note To set trunk characteristics, the interface must be in trunk mode.

The following example shows how to allow trunking on specified VLANs:

```
Router(config)# interface ucse 1/0/0
Router(config-if)# switchport mode trunk
Router(config-if)# switchport trunk allowed vlan 1-2,40,60,1002-1005
```

Related Commands

Command	Description
show interfaces switchport	Displays administrative and operational status of a switching (nonrouting) port.
vlan dot1q tag native	Enables dot1q tagging for all VLANs in a trunk.

switchport vlan mapping

To map the traffic arriving on the VLAN original-vlan-id to the VLAN translated-vlan-id and the traffic that is internally tagged with the VLAN translated-vlan-id with the VLAN original-vlan-id before leaving the port, use the **switchportvlanmapping** command in interface configuration mode. To clear the mapping between a pair of VLANs or clear all the mappings that are configured on the switch port, use the **no** form of this command.

switchport vlan mapping *original-vlan-id translated-vlan-id*
no switchport vlan mapping {*original-vlan-id translated-vlan-id* | **all**}

Syntax Description

original-vlan-id	Original VLAN number; valid values are from 1 to 4094.
translated-vlan-id	Translated VLAN number; valid values are from 1 to 4094.
all	Clears all the mappings that are configured on the switch port.

Command Default

No mappings are configured on any switch port.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(17b)SXA	Support for this command was introduced on the Supervisor Engine 720.
12.2(18)SXE	This command is not supported on GE Layer 2 WAN ports.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

This command is not supported on GE Layer 2 WAN ports.

You must enable VLAN translation on the port where you want VLAN translation to work. Use the **switchportvlanmappingenable** command to enable VLAN translation.

Do not remove the VLAN that you are translating from the trunk. When you map VLANs, make sure that both VLANs are allowed on the trunk that carries the traffic.

The table below lists the VLAN translation, the type of VLAN translation support, the number of ports that you can configure per port group, and the trunk type for each module that supports VLAN translation.

Table 284: Modules That Support VLAN Translation

Product Number	VLAN Translation Support Type	Number of Port Groups	Port Ranges per Port Group	Translations per Port Group	VLAN Translation Trunk-Type Support
WS-SUP720	Per port group	1	1-2	32	802.1Q
WS-X6704-10GE	Per port	4	1 port in each group	128	ISL and 802.1Q
WS-X6501-10GEX4	Per port	1	1 port in 1 group	32	802.1Q

Product Number	VLAN Translation Support Type	Number of Port Groups	Port Ranges per Port Group	Translations per Port Group	VLAN Translation Trunk-Type Support
WS-X6502-10GE	Per port	1	1 port in 1 group	32	802.1Q
WS-X6724-SFP	Per port group	2	1-12, 13-24	128	ISL and 802.1Q
WS-X6816-GBIC	Per port group	4	1-8, 9-16	32	802.1Q
WS-X6516A-GBIC	Per port group	2	1-8, 9-16	32	802.1Q
WS-X6516-GBIC	Per port group	2	1-8, 9-16	32	802.1Q
WS-X6748-GE-TX	Per port group	4	1-12, 13-24, 25-36, 37-48	128	ISL and 802.1Q
WS-X6516-GE-TX	Per port group	2	1-8, 9-16	32	802.1Q
WS-X6524-100FX-MM	Per port group	1	1-24	32	ISL and 802.1Q
WS-X6548-RJ-45	Per port group	1	1-48	32	ISL and 802.1Q
WS-X6548-RJ-21	Per port group	1	1-48	32	ISL and 802.1Q

The mapping that you configured using the **switchportvlanmapping** command does not become effective until the switch port becomes an operational trunk port.

The VLAN mapping that is configured on a port may apply to all the other ports on the same ASIC. In some cases, a mapping that is configured on one of the ports on an ASIC can overwrite a mapping that is already configured on another port on the same ASIC.

The port VLAN mapping is applied to all the ports on a port ASIC if that ASIC does not support per-port VLAN mapping.

If you configure VLAN mapping on the port ASIC that is a router port, the port-VLAN mapping does not take effect until the port becomes a switch port.

You can map any two VLANs regardless of the trunk types carrying the VLANs.

Examples

This example shows how to map the original VLAN to the translated VLAN:

```
Router(config-if)#
 switchport vlan mapping 100 201
```

This example shows how to clear the mappings that are between a pair of VLANs:

```
Router(config-if)#
 no switchport vlan mapping 100 201
```

This example shows how to clear all the mappings that are configured on the switch port:

```
Router(config-if)#
 no switchport vlan mapping all
```

Related Commands

Command	Description
show interfaces vlan mapping	Display the status of a VLAN mapping on a port.
show vlan mapping	Registers a mapping of an 802.1Q VLAN to an ISL VLAN.
switchport vlan mapping enable	Enables VLAN mapping per switch port.

switchport vlan mapping enable

To enable VLAN mapping per switch port, use the **switchportvlanmappingenable** command in interface configuration mode. To disable VLAN mapping per switch port, use the **no** form of this command.

switchport vlan mapping enable
no switchport vlan mapping enable

Syntax Description

This command has no arguments or keywords.

Command Default

VLAN mapping is disabled on all switch ports.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(17b)SXA	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Note You must enter the **switchportvlanmappingenable** command on the port where you want the mapping to take place.

The switchport vlan mapping enable command enables or disables VLAN-mapping lookup in the hardware regardless of whether the mapping is configured by the global VLAN mapping command or the switchport VLAN mapping command.

This command is useful on the hardware that supports VLAN mapping per ASIC only because you can turn on or off VLAN translation selectively on ports that are connected to the same port ASIC.

Examples

This example shows how to enable VLAN mapping per switch port:

```
Router(config-if)#
 switchport vlan mapping enable
```

This example shows how to disable VLAN mapping per switch port:

```
Router(config-if)#
 no switchport vlan mapping enable
```

Related Commands

Command	Description
show interfaces vlan mapping	Displays the status of a VLAN mapping on a port.
show vlan mapping	Registers a mapping of an 802.1Q VLAN to an ISL VLAN.

Command	Description
switchport vlan mapping	Maps the traffic arriving on the VLAN original-vlan-id to the VLAN translated-vlan-id and the traffic that is internally tagged with the VLAN translated-vlan-id with the VLAN original-vlan-id before leaving the port.

switchport voice vlan

To configure a voice VLAN on a multiple-VLAN access port, use the **switchportvoicevlan** command in interface configuration mode. To remove the voice VLAN from the switch port, use the **no** form of the command.

switchport voice vlan {*vlan-id* | **dot1p** | **none** | **untagged**}
no switchport voice vlan

Syntax Description

vlan id	Voice VLAN identifier (VVID) of the VLAN used for voice traffic. Valid IDs are from 1 to 1005 (IDs 1006 to 4096 are not supported). Do not enter leading zeros. The switch port is an 802.1Q trunk port.
dot1p	The telephone uses priority tagging and uses VLAN 0. The switch port is an 802.1Q trunk port.
none	The telephone is not instructed through the command line interface (CLI) about the voice VLAN. The telephone uses its own configuration from the telephone keypad and transmits untagged voice traffic in the default VLAN.
untagged	The telephone does not tag frames; it uses VLAN 4095. The switch port can be an access port or an 802.1Q trunk port.

Command Default

The switch default is to not automatically configure the telephone (**none**).

The Cisco IP 7960 telephone default is to generate an 802.1Q/802.1P frame.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)XT	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T to support creation of switchports .
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX and introduced on the Supervisor Engine 720.
12.2(17d)SXB	This command was integrated into Cisco IOS Release 12.2(17d)SXB and introduced on the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

This command does not create a voice VLAN. You can create a voice VLAN in VLAN-configuration mode by entering the **vlan(globalconfigurationmode)** command. If you configure both the native VLAN and the voice VLAN in the VLAN database and set the switch port to multiple-VLAN access mode, this command brings up the switch port as operational.

If you enter a voice VLAN identifier, the switch port sends CDP packets that configure the IP phone to transmit voice traffic in the voice VLAN in 802.1Q frames that are tagged with a Layer 2 CoS value . The default Layer 2 CoS is 5. The default Layer 3 IP-precedence value is 5.

If you enter dot1p, the switch port sends CDP packets that configure the IP phone to transmit voice traffic in the default VLAN in 802.1p frames that are tagged with a Layer 2 CoS value.

If you enter none, the switch port does not send CDP packets with VVID TLVs.

If you enter **untagged**, the switch port is enabled to receive untagged packets only.

Examples

This example shows how to create an operational multiple-VLAN access port with VLAN 101 as the voice VLAN:

```
Router(config-if)# switchport
Router(config-if)# switchport mode access
Router(config-if)# switchport access vlan 100
Router(config-if)# switchport voice vlan 101
Router(config-if)
```

This example shows how to change the multiple-VLAN access port to a normal access port:

```
Router(config-if)# interface fastethernet5/1
Router(config-if)# no switchport voice vlan
Router(config-if)
```

Related Commands

Command	Description
switchport access vlan	Sets the VLAN when the interface is in access mode.
switchport mode	Sets the interface type.

sync interval

To specify an interval for the device to exchange Precision Time Protocol synchronization messages, use the **sync interval** command in PTP port configuration mode. To disable a sync interval configuration, use the **no** form of this command.

sync interval *interval-value*
no sync interval *interval-value*

Syntax Description

interval-value	Value of the interval at which the device sends sync packets. The intervals are set using log base 2 values, as follows: • 4—1 packet every 16 seconds • 3—1 packet every 8 seconds • 2—1 packet every 4 seconds • 1—1 packet every 2 seconds • 0—1 packet every second • -1—1 packet every 1/2 second, or 2 packets per second • -2—1 packet every 1/4 second, or 4 packets per second • -3—1 packet every 1/8 second, or 8 packets per second • -4—1 packet every 1/16 seconds, or 16 packets per second • -5—1 packet every 1/32 seconds, or 32 packets per second • -6—1 packet every 1/64 seconds, or 64 packets per second The recommended value is -6.

Command Default

The default value is 1.

Command Modes

PTP port configuration (config-ptp-port)

Command History

Release	Modification
15.0(1)S	This command was introduced.

Examples

The following example shows how to configure the PTP sync interval:

```
Device> enable
Device# configure terminal
Device(config)# ptp clock ordinary domain 0
Device(config-ptp-clk)# clock-port slave slaveport
Device(config-ptp-port)# sync interval -4
Device(config-ptp-port)# end
```

Related Commands

Command	Description
clock-port	Specifies the mode of a PTP clock port.

sync-restart-delay

To set the synchronization-restart delay timer to ensure accurate status reporting, use the **sync-restart-delay** command in interface configuration mode. To disable the synchronization-restart delay timer, use the **no** form of this command.

sync-restart-delay *timer*
no sync-restart-delay *timer*

Syntax Description

timer	Interval between status-register resets; valid values are from 200 to 60000 milliseconds.

Command Default

timer is **210** milliseconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported on Gigabit Ethernet fiber ports only.

The status register records the current status of the link partner.

Examples

This example shows how to set the Gigabit Ethernet synchronization-restart delay timer:

```
Router(config-if)# sync-restart-delay 2000
```

Related Commands

Command	Description
show running-config	Displays the status and configuration of the module or Layer 2 VLAN.

syscon address

To specify the system controller for a managed shelf, use the **sysconaddress** command in global configuration mode. To stop the management of the shelf by the system controller, use the **no** form of this command.

syscon address *ip-address password*
no syscon address

Syntax Description

ip-address	IP address of the system controller.
password	Password string.

Command Default

No system controller is specified.

Command Modes

Global configuration

Command History

Release	Modification
11.3AA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is required in order for the shelf to be managed by the system controller.

Examples

The following example configures a shelf to be managed by a system controller at 10.2.3.4 using the password green:

```
Router# syscon address 10.2.3.4 green
```

Related Commands

Command	Description
show syscon sdp	Displays information about the Shelf Discovery Protocol.
syscon source-interface	Specifies the interface to use for the source address in SDP packets.

syscon shelf-id

To specify a shelf ID for a managed shelf, use the **sysconshelf-id**command in global configuration mode. To remove the shelf ID, use the **no** form of this command.

syscon shelf-id *number*
no syscon shelf-id

Syntax Description

number	Shelf ID. The value ranges from 0 to 9999.

Command Default

No shelf ID is specified.

Command Modes

Global configuration

Command History

Release	Modification
11.3AA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to specify a shelf ID for a managed shelf. Some platforms, such as the Cisco AS5800, use other commands to assign a shelf ID. In these situations, do not specify a shelf ID with the **sysconshelf-id** command. Use the platform-specific command instead.

Examples

The following example configures a shelf ID of 5 for the managed shelf:

```
Router# syscon shelf-id 5
```

Related Commands

Command	Description
show syscon sdp	Displays information about the Shelf Discovery Protocol.
syscon address	Specifies the system controller for a managed shelf.

syscon source-interface

To specify the interface to use for the source address in Shelf Discovery Protocol (SDP) packets, use the **sysconsource-interface**command in global configuration mode. To return to the default source interface for a packet (the interface that sent the packet from the shelf), use the **no** form of this command.

syscon source-interface *type number*
no syscon source-interface

Syntax Description

type number	Type and number of the interface to use for the source IP address.

Command Default

SDP packets use the IP address of the output interface.

Command Modes

Global configuration

Command History

Release	Modification
11.3AA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to ensure that all SDP packets sent by the managed shelf have the same source IP address.

Examples

The following example configures a shelf to use the IP address of Ethernet interface 99/1/0:

```
Router# syscon source-address Ethernet99/1/0
```

Related Commands

Command	Description
show syscon sdp	Displays information about the Shelf Discovery Protocol.
syscon shelf-id	Specifies a shelf ID for a managed shelf.

system flowcontrol bus

To set the FIFO overflow error count, use the **system flowcontrol bus** command in global configuration mode. To return to the original FIFO threshold settings, use the **no** form of this command.

[**default**] **system flowcontrol bus** {**auto** | **on**}
no system flowcontrol bus

Syntax Description

default	(Optional) Specifies the default settings.
auto	Monitors the FIFO overflow error count and sends a warning message if the FIFO overflow error count exceeds a configured error threshold in 5-second intervals.
on	Specifies the original FIFO threshold settings.

Command Default

auto

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXF	Support for this command was introduced on the Supervisor Engine 720 and the Supervisor Engine 32.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Note We recommend that you leave the system flow control in auto mode and use the other modes under the advice of Cisco TAC only.

Examples

This example shows how to monitor the FIFO overflow error count and send a warning message if the FIFO overflow error count exceeds a configured error threshold in 5-second intervals:

```
Router(config)# system flowcontrol bus auto
```

This example shows how to specify the original FIFO threshold settings:

```
Router(config)# system flowcontrol bus on
```

system jumbomtu

To set the maximum size of the Layer 2 and Layer 3 packets, use the system **jumbo**mtu command in global configuration mode. To revert to the default MTU setting, use the **no** form of this command.

system jumbomtu mtu-size
no system jumbomtu

Syntax Description

mtu-size	Maximum size of the Layer 2 and Layer 3 packet s; valid values are from 1500 to 9216 bytes.

Command Default

mtu-size is **9216** bytes.

Command Modes

Global configuration

Command History

Release	Modification
1.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The *mtu-size* parameter specifies the Ethernet packet size, not the total Ethernet frame size. The Layer 3 MTU is changed as a result of entering the **system jumbo**mtucommand.

The **system jumbo**mtucommand enables the global MTU for port ASICs. On a port ASIC after jumbo frames are enabled, the port ASIC accepts any size packet on the ingress side and checks the outgoing packets on the egress side. The packets on the egress side that exceed the global MTU are dropped by the port ASIC.

For example, if you have port A in VLAN 1 and Port B in VLAN 2, and if VLAN 1 and VLAN 2 are configured for **mtu 9216** and you enter the **system jumbomtu 4000** command, the packets that are larger than 4000 bytes are not transmitted out because Ports B and A drop anything larger than 4000 bytes.

Examples

This example shows how to set the global MTU size to 1550 bytes:

```
Router(config)# system jumbomtu 1550
```

This example shows how to revert to the default MTU setting:

```
Router(config)# no system jumbomtu
```

Related Commands

Command	Description
mtu	Adjusts the maximum packet size or MTU size.
show interfaces	Displays traffic that is seen by a specific interface.
show system jumbomtu	Displays the g lobal MTU setting.

t1 through tug-2 e1 unframed

t1

To create a logical T1 controller from each of the specified time slots of the T3 line, use the **t1**command in controller configuration mode. To delete the defined logical controller, use the **no** form of this command.

t1 *ds1* **controller**
no t1 *ds1* **controller**

Syntax Description

ds1	Time slot within the T3 line. The valid time-slot range is from 1 to 28.

Command Default

No default behavior or values.

Command Modes

Controller configuration

Command History

Release	Modification
11.3AA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The purpose of this command is to convert the collection of the 28 T1 controllers comprising the T3 controller into individual T1 controllers that the system can use. In other words, the Cisco AS5800 access server cannot pass data until a T1 controller is configured (using the **controller** command), and you cannot configure a T1 controller until it has been created using the **t1** command.

Examples

The following example shows how to configure a logical T1 controller at T1 time slot 1 for the T3 controller located in shelf 1, slot 4, port 0. Note that you have to enter the command from controller configuration mode.

```
Router(config)# controller
 t3 1/4/0
Router(config-controller)# t1 1 controller
Router(config-controller)# end
```

Related Commands

Command	Description
controller	Configures a T1 and other types of controller and enters controller configuration mode.
controller t3	Configures a T3 controller.

t1 bert

To enable or disable a bit error rate tester (BERT) test pattern for a T1 channel on the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers, use the **t1bert**command in controller configuration mode. To disable a BERT test pattern, use the **no** form of this command.

t1 *channel* **bert pattern** {**0s** | **1s** | **2^15** | **2^20** | **2^23**} **interval** *minutes* [**unframed**]
no t1 *channel* **bert pattern** {**0s** | **1s** | **2^15** | **2^20** | **2^23**} **interval** *minutes* [**unframed**]

Syntax Description

channel	Number between 1 and 28 that indicates the T1 channel.
pattern	Specifies the length of the repeating BERT test pattern.
0s	0s--Repeating pattern of zeros (...000...).
1s	1s--Repeating pattern of ones (...111...).
2^15	215--Pseudorandom repeating pattern that is 32,767 bits in length.
2^20	220--Pseudorandom repeating pattern that is 1,048,575 bits in length.
2^23	223--Pseudorandom repeating pattern that is 8,388,607 bits in length.
interval *minutes*	Specifies the duration of the BERT test, in minutes. The interval can be a value from 1 to 14400.
unframed	(Optional) Specifies T1 unframed BERT.

Command Default

No BERT test is performed.

Command Modes

Controller configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2S	The **unframed** keyword was added to this command.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The BERT test patterns from the CT3IP are framed test patterns (that is, the test patterns are inserted into the payload of the framed T1 signal).

To view the BERT results, use the **showcontrollert3** or **showcontrollert3brief** EXEC commands. The BERT results include the following information:

- Type of test pattern selected
- Status of the test

- Interval selected
- Time remaining on the BERT test
- Total bit errors
- Total bits received

When the T1 channel has a BERT test running, the line state is DOWN. Also, when the BERT test is running and the Status field is Not Sync, the information in the total bit errors field is not valid. When the BERT test is done, the Status field is not relevant.

The**t1bert**command is not written to NVRAM because it is only used for testing the T1 channel for a short predefined interval and for avoiding accidentally saving the command, which could cause the interface not to come up the next time the router reboots.

Note T1 channels on the CT3IP are numbered 1 to 28 rather than the more traditional zero-based scheme (0 to 27) used with other Cisco products. This numbering scheme ensures consistency with telco numbering schemes for T1 channels within channelized T3 equipment.

Examples

The following example shows how to run a BERT test pattern of all zeros for 30 minutes on T1 channel 6 on the CT3IP in slot 9:

```
Router(config
)
# controller t3 9/0/0
Router(config
-controller)
# t1 6 bert pattern 0s interval 30
```

Related Commands

Command	Description
show controllers t3	Displays the hardware and software driver information for a T3 controller.

t1/e1 cem-group

To create a circuit emulation (CEM) channel from one or more time slots of a T1/E1 ports on the Channelized T3/E3 Interface Module, use the **t1/e1cem-group** command in controller configuration mode.

t1/e1 *channel* **cem-group***cem-group-id***unframed**

Syntax Description

channel	Number between 1 and 28 that indicates the T1 channel.
cem-group-id	Specifies the cem circuit number to be used for the cem circuit. This number must be unique across all cem-circuits.
unframed	Specifies that a single CEM channel is being created including all time slots and the framing structure of the line. This unframed keyword is used to create an SAToP circuit.

Command Default

No CEM groups are defined.

Command Modes

Controller configuration

Command History

Command History

Release	Modification
XE 3.18SP	This command was introduced.
XE Everest 16.5.1	This command was introduced on the Cisco NCS 4200 Series and Cisco ASR 900 Series Routers.

Usage Guidelines

Use this command to configure cem-group for channelized T1/E1 under T3/E3 controller.

Examples

The following example shows how to create cem-group on the Channelized T3 Interface Module:

```
Router(config-controller)# t1 1 cem-group 0 unframed
```

Examples

The following example shows how to create cem-group on the Channelized E3 Interface Module:

```
Router(config-controller)# e1 1 cem-group 0 unframed
```

t1 clock source

To specify where the clock source is obtained for use by each T1 channel on the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers, use the **t1clocksource** command in controller configuration mode.

t1 *channel* **clock source** {**internal** | **line**}

Syntax Description

channel	Number between 1 and 28 that indicates the T1 channel.
internal	Specifies that the internal clock source is used. This is the default.
line	Specifies that the network clock source is used.

Command Default

Internal

Command Modes

Controller configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If you do not specify the **t1clocksource**command, the default clock source of **internal** is used by all the T1s on the CT3IP.

You can also set the clock source for the CT3IP by using the **clocksource**(CT3IP)controller configuration command.

Note T1 channels on the CT3IP are numbered 1 to 28 rather than the more traditional zero-based scheme (0 to 27) used with other Cisco products. This numbering scheme ensures consistency with telco numbering schemes for T1 channels within channelized T3 equipment.

This command does not have a **no** form.

Examples

The following example shows how to set the clock source to line T1 6 and T1 8 on the CT3IP:

```
Router(config
)
# controller t3 9/0/0
Router(config
-controller)
# t1 6 clock source line
Router(config
```

```
-controller)
# t1 8 clock source line
```

Related Commands

Command	Description
clock source (CT3IP)	Specifies where the clock source is obtained for use by the CT3IP in Cisco 7500 series routers.

t1 external

To specify that a T1 channel on the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers is used as an external port so that the T1 channel can be further multiplexed on the Multichannel Interface Processor (MIP) or other multiplexing equipment, use the **t1external**command in controller configuration mode. To remove a T1 as an external port, use the **no** form of this command.

t1 external *channel* [**cablelength** *feet*] [**linecode** [{**ami** | **b8zs**}]]
no t1 external *channel*

Syntax Description

channel	Number 1, 2, or 3 that indicates the T1 channel.
cablelength *feet*	(Optional) Specifies the cable length, in feet, from the T1 channel to the external CSU or MIP. Values are from 0 to 655. Default is 133.
linecode ami | **b8zs**	(Optional) Specifies the line coding used by the T1. Values are alternate mark inversion (AMI) or bipolar 8 zero suppression (B8ZS). Default is B8ZS.

Command Default

No external T1 is specified. The default cable length is 133 feet. The default line coding is B8ZS.

Command Modes

Controller configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The first three T1 channels (1, 2, and 3) of the CT3IP can be broken out to the DSUP-15 connectors on the CPT3IP so that the T1 channel can be further demultiplexed by the MIP on the same router or on another router.

After you configure the external T1 channel, you can continue configuring it as a channelized T1 (also referred to as a *fractional* T1) from the MIP. All channelized T1 commands might not be applicable to the T1 interface. After you configure the channelized T1 on the MIP, you can continue configuring it as you would a normal serial interface. All serial interface commands might not be applicable to the T1 interface.

The line coding on the T1 channel and the MIP must be the same. Because the default line coding format on the T1 channel is B8ZS and the default line coding on the MIP is AMI, you must change the line coding on the MIP or on the T1 so that they match.

To determine if the external device connected to the external T1 port is configured and cabled correctly before configuring an external port, use the **showcontrollerst3** command and locate the line Ext1... in the display output. The line status can be one of the following:

- LOS--Loss of signal indicates that the port is not receiving a valid signal. This is the expected state if nothing is connected to the port.

- AIS--Alarm indication signal indicates that the port is receiving an all-ones signal.
- OK--A valid signal is being received and the signal is not an all-ones signal.

Note T1 channels on the CT3IP are numbered 1 to 28 rather than the more traditional zero-based scheme (0 to 27) used with other Cisco products. This numbering scheme ensures consistency with telco numbering schemes for T1 channels within channelized T3 equipment.

Note Although you can specify a cable length from 0 to 655 feet, the hardware only recognizes the following ranges: 0 to 133, 134 to 266, 267 to 399, 400 to 533, and 534 to 655. For example, entering 150 feet uses the 134 to 266 range. If you later change the cable length to 200 feet, there is no change because 200 is within the 134 to 266 range. However, if you change the cable length to 399, the 267 to 399 range is used. The actual number you enter is stored in the configuration file.

Examples

The following example shows how to configure T1 1 on the CT3IP as an external port using AMI line coding and a cable length of 300 feet:

```
Router(config
)
# controllers t3 9/0/0
Router(config
-controller)
# t1 external 1 cablelength 300 linecode ami
```

Related Commands

Command	Description
show controllers t3	Displays the hardware and software driver information for a T3 controller.

t1 fdl ansi

To enable the 1-second transmission of the remote performance reports via the Facility Data Link (FDL) per ANSI T1.403 for a T1 channel on the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers, use the **t1fdlansi** command in controller configuration mode. To disable the performance report, use the **no** form of this command.

t1 *channel* **fdl** **ansi**
no **t1** *channel* **fdl** **ansi**

Syntax Description

channel	Number between 1 and 28 that indicates the T1 channel.

Command Default

Disabled

Command Modes

Controller configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The**t1fdlansi** command can be used only if the T1 framing type is Extended Super Frame (ESF).

To display the remote performance report information, use the**showcontrollerst3remoteperformance** command.

Note T1 channels on the CT3IP are numbered 1 to 28 rather than the more traditional zero-based scheme (0 to 27) used with other Cisco products. This numbering scheme ensures consistency with telco numbering schemes for T1 channels within channelized T3 equipment.

Examples

The following example shows how to generate the performance reports for T1 channel 8 on the CT3IP:

```
Router(config
)
# controller t3 9/0/0
Router(config
-controller)
# t1 8 fdl ansi
```

Related Commands

Command	Description
show controllers t3	Displays the hardware and software driver information for a T3 controller.

t1 framing

To specify the type of framing used by T1 channels, use the**t1framing** command in controller configuration mode.

Cisco 7500 Series Routers with Channelized T3 Interface Processor
t1 *channel* **framing** {**esf** | **sf**}

Channelized T3 Shared Port Adapters
t1 channel framing {**esf** | **sf** [**hdlc-idle** {**0x7e** | **0xff**}] [**mode j1**]}
no t1 channel framing {**esf** | **sf** [**hdlc-idle** {**0x7e** | **0xff**}] [**mode j1**]}

Syntax Description

channel	Number indicating the T1 channel. • On the CT3IP--1 to 28 • On the 2-Port and 4-Port Channelized T3 SPA --0 to 23
esf	Specifies that Extended Super Frame (ESF) is used as the T1 framing type. This is the default for the CT3IP.
sf	Specifies that Super Frame (SF) is used as the T1 framing type. This is the default for the 2-Port and 4-Port Channelized T3 SPA.
hdlc-idle {**0x7e** | **0xff**}	(Optional) Sets the idle pattern for the T1 interface to either **0x7e** (the default) or **0xff**.
mode {**j1**}	(Optional) Specifies the JT-G704 Japanese frame type. The mode keyword is not supported on Cisco 7304 routers with the 2-Port and 4-Port Channelized T3 SPA.

Command Default

esf (for C3TIP)

sf (for 2-Port and 4-Port Channelized T3 SPA)

Command Modes

Controller configuration

Command History

Release	Modification
11.3	This command was introduced.
12.0(14)S	This command was integrated into Cisco IOS Release 12.0(14)S. The **hdlc-idle** keyword option was added.
12.2S	This command was integrated into Cisco IOS Release 12.2S.
12.2(25)S3	This command was integrated into Cisco IOS Release 12.2(25)S3 to support SPAs on the Cisco 7304 series routers.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE to support SPAs on the Cisco 7600 series router and Catalyst 6500 series switch. The **mode** keyword option was added.

Release	Modification
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S to support SPAs on the Cisco 12000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If you do not specify the **t1framing**command, the default ESF is used.

Note T1 channels on the CT3IP are numbered 1 to 28 rather than the more traditional zero-based scheme (0 to 27) used with other Cisco products. This numbering scheme ensures consistency with telco numbering schemes for T1 channels within channelized T3 equipment.

To return to the default mode, use the no form of this command. This command does not have a **no** form on the Cisco 7500 series router with the CT3IP.

The mode keyword is not supported on Cisco 7304 routers with the 2-Port and 4-Port Channelized T3 SPA.

Examples

The following example shows how to set the framing for the T1 6 and T1 8 on the CT3IP to Super Frame:

```
Router(config
)
# controller t3 9/0/0
Router(config
-controller)
# t1 6 framing sf
Router(config
-controller)
# t1 8 framing sf
```

Related Commands

Command	Description
controller	Configures a T1, E1, or T3 controller and enters controller configuration mode.
show controller	Displays controller configuration.

t1 linecode

To specify the type of line coding used by the T1 channels on the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers, use the **t1linecode**command in controller configuration mode.

t1 *channel* **linecode** [{**ami** | **b8zs**}]

Syntax Description

channel	Number between 1 and 28 that indicates the T1 channel.
ami	Specifies that alternate mark inversion (AMI) line coding is used by the T1 channel.
b8zs	Specifies that bipolar 8 zero suppression (B8ZS) line coding is used by the T1 channel. This is the default.

Command Default

B8ZS

Command Modes

Controller configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If you do not specify the **t1linecode**command, the default B8ZS is used.

AMI Line Coding

If you select **ami** line coding for the T1 channel, you must also invert the data on the T1 channel by using the **invertdata** interface command. This is required because the T1 channel is bundled into the T3 signal, so there are no local T1 line drivers and receivers associated with it. Therefore, the **t1***channel***linecodeami** command does not modify local line driver settings. Rather, it advises the CT3IP what line code the remote T1 is using. The CT3IP uses this information solely for the purpose of determining whether or not to enable the pulse density enforcer for that T1 channel.

B8ZS Line Coding

When you select **b8zs** line coding, the pulse density enforcer is disabled. When you select **ami** line coding, the pulse density enforcer is enabled. To avoid having the pulse density enforcer corrupt data, the T1 channel should be configured for inverted data.

Note T1 channels on the CT3IP are numbered 1 to 28 rather than the more traditional zero-based scheme (0 to 27) used with other Cisco products. This numbering scheme ensures consistency with telco numbering schemes for T1 channels within channelized T3 equipment.

Examples

The following example shows how to set the line coding for T1 channel 16 on the CT3IP to AMI:

```
Router(config
)
# controller t3 9/0/0
Router(config
-controller)
# t1 16 linecode ami
Router(config
-controller)
# exit
Router(config
)
# interface serial 9/0/0:16
Router(config
-if)
# invert data
```

Related Commands

Command	Description
invert data	Inverts the data stream.
loopback remote (interface)	Loops packets through a CSU/DSU, over a DS3 link or a channelized T1 link, to the remote CSU/DSU and back.

t1 logging-events

To print typical T1 controller Up and Down messages on a channelized T3 port adapterin T3 controller, use the t1 **logging-eventscommand**configuration mode**.TodisableprintingoftheT1controllerUpandDownmessages,usethenoformofthiscommand.**

t1 t1 logging-events [**detail**]
[**no**] **t1 t1 logging-events**

Syntax Description

t1	Number between 1 and 28 that represents the T1 channel for the Channelized T3 Interface Processor (CT3IP) on Cisco 7500 series and Cisco 7200 series routers.
detail	(Optional) Enables printing the reason code when a T1 controller of a T3 controller changes from the Up state to the Down state.

Command Default

The **t1logging-eventscommandisthedefault.**

Command Modes

T3 controller configuration mode.

Command History

Release	Modification
12.2(19c)	This command was introduced.

Usage Guidelines

This command refers to the T1 controller as part of a T3 controller.

The no t1 logging-events command disables printing of the controller Up and Down messages. These messages will appear neither on the console nor in the logs.

Examples

The following example uses the **t1logging-events**command to print normal controller Up and Down messages, without indicating the reason code for a changed state. The T1 1 controller is part of the T3 controller with a bay/port of 4/1.

```
Router(config-controller)# t1 1 logging-events
*Jun 20 00:29:39: %CONTROLLER-5-UPDOWN: Controller T3 4/1 T1 1, changed state to UP
*Jun 20 00:30:09: %CONTROLLER-5-UPDOWN: Controller T3 4/1 T1 1, changed state to DOWN
```

The following example uses the **t1logging-eventsdetail**command to show the Out-of-Frame (OOF) reason code when the T1 1 controller of a T3 controller with a bay/port of 4/1 changes from an Up state to a Down state:

```
Router(config-controller)# t1 1 logging-events detail
*Jun 19 17:47:50: %CONTROLLER-5-DOWNDETAIL: Controller T3 4/1 T1 1, changed state to down
due to OOF
```

Related Commands

Command	Description
logging-events	**Prints typical T3 controller Up and Down messages** on a channelized T3 port adapter**.**

t1/e1 loopback

To set the loopback method for testing T1, E1, T3 or E3 interface module, use the **t1loopback** command in controller configuration mode. To remove the existing loopback, use the no form of this command.

t1 *t1 number* **loopback** { *local* | *network* { *line* | *payload* } }

e1 *e1 number* **loopback** { *local* | *network* { *line* | *payload* } }

Syntax Description

t1 number	Displays the T1 channel number. It ranges from 1-28.
e1 number	Displays the E1 channel number. It ranges from 1-16.
local	Places the interface into local loopback mode and creates a loopback wherein information received from the locally-attached customer premises equipment (CPE) is transmitted back to the locally-attached CPE.
network	Creates a loopback wherein data received over the network from the remote CPE is transmitted back to the remote CPE. • payload: Creates a loopback of only the data in individual time slots. In this mode, framing bits are terminated and then regenerated instead of being looped back. This mode is not available if the port is configured for framing unframed. • line: Creates a full physical layer loopback of all bits, including data and framing bits.

Command Default

No loopback is configured

Command Modes

Controller configuration

Command History

Command History

Release	Modification
XE 3.18SP	This command was introduced on the Cisco NCS 4200 series.
XE Everest 16.5.1	This command was integrated into Cisco NCS 4200 Series and Cisco ASR 900 Series Routers.

Examples

The following example shows how to create the local loopback on the controller :

```
Router(config-controller)# t1 1 loopback local
```

The following example shows how to create a network line loopback on a controller.

```
Router(config-controller)# t1 1 loopback network line
```

Examples

The following example shows how to create the local loopback on the controller :

```
Router(config-controller)# e1 1 loopback local
```

Related Commands

Command	Description
controller	Enters controller configuration mode.
show controller t3	Displays the information about T3 controller.

t1 t1-line-number cem-group

To create a single Structure-Agnostic TDM over Packet (SAToP) CEM group, use the **t1** *t1-line-number* **cem-group** command in controller configuration mode.

t1 *t1-line-number* **cem-group** *cem-group-number* **unframed**

Syntax Description

t1-line-number	Specifies the T1 line number. The range is 1 to 4.
cem-group-number	The **cem-group-number** keyword identifies the channel number to be used for this channel. For T1 ports, the range is 0 to 23. For E1 ports, the range is 0 to 30.
unframed	Use the **unframed** keyword to specify that a single CEM channel is being created including all time slots and the framing structure of the line. It assigns all the T1 timeslots to the CEM channel.

Command Default

None

Command Modes

Controller configuration

Command History

Release	Modification
XE 3.18 SP	Support for this command was introduced on NCS 4200 Series.

Usage Guidelines

The command is used to configure t1 channels under CT3 mode. You can configure 28 T1 channels with CT3 mode.

Examples

The following example shows how to configure DS1 CT3 SAToP mode :

```
enable
configure terminal
controller Mediatype 0/5/0
mode sonet
controller sonet 0/5/0
rate oc12
sts-1 1
mode ct3
t1 1 cem-group 100 unframed
interface cem 0/5/0
no ip address
cem 100
xconnect 2.2.2.2 10 encapsulation mpls
exit
```

Related Commands

Command	Description
controller sonet	Displays information about Synchronous Optical Network (SONET) controllers.
show controller sonet	Displays SONET controller configuration.

t1 t1-line-number clock source

To specify where the clock source is obtained for use by each T1 channel, use the **t1** *t1-line-number* **clock source** command in controller configuration mode.

t1 *t1-line-number* **clock source** {*internal* | *line*}

Syntax Description

Syntax Description

t1-line-number	Specifies the T1 line number. The range is 1 to 4.
internal	Specifies that the internal clock source is used. This is the default.
line	Specifies that the network clock source is used.

Command Default

The default mode is internal.

Command Modes

Controller configuration

Command History

Release	Modification
XE 3.18 SP	Support for this command was introduced on NCS 4200 Series.

Usage Guidelines

If you do not specify the **t1 clock source** command, the default clock source of internal is used by all the T1s. The no form of this command is available for clock source line mode.

Examples

The following example shows how to configure DS1 CT3 SAToP mode:

```
enable
configure terminal
controller MediaType 0/5/0
mode sonet
controller sonet 0/5/0
rate oc12
sts-1 1
mode ct3
t1 1 cem-group 100 unframed
t1 1 framing unframed
t1 1 clock source internal
end
```

Related Commands

Command	Description
controller sonet	Configures a T1, E1, or T3 controller and enters controller configuration mode.
show controller sonet	Displays controller configuration.

t1 t1 line-number framing

To specify the type of framing used by T1 channels, use the **t1** *t1-line-number* **framing** command in controller configuration mode.

t1 *t1-line-number* **framing** {*esf* | *sf* | *unframed*}

Syntax Description

Syntax Description

t1-line-number	The name of a CEM interface parameters class.
esf	Specifies that Extended Super Frame (ESF) is used as the T1 framing type.
sf	Specifies that Super Frame (SF) is used as the T1 framing type.
unframed	Creates an unframed (clear channel) logical channel group on a T1 line.

Command Default

None

Command Modes

Controller configuration

Command History

Release	Modification
XE 3.18SP	Support for this command was introduced on NCS 4200 Series.

Usage Guidelines

If you do not specify the **t1** *t1-line-number* **framing** command, the default ESF is used.

Examples

The following example shows how to configure DS1 CT3 SAToP mode:

```
enable
configure terminal
controller MediaType 0/5/0
mode sonet
controller sonet 0/5/0
rate oc12
sts-1 1
mode ct3
t1 1 cem-group 100 unframed
t1 1 framing unframed
exit
```

Related Commands

Command	Description
controller sonet	Configures a T1, E1, or T3 controller and enters controller configuration mode.
show controller sonet	Displays controller configuration.

t1 span

To enable link noise monitoring on a clear channel T1 link on Cisco 10000 series routers, use the **t1span** command in controller configuration mode. To disable link noise monitoring, use the **no** form of this command.

t1 *channel* **span** {**minor-warn** | **remove** | **major-warn**} [{**duration** *seconds* | **lcv** *threshold* [**pcv** *threshold*] [{**set** | **clear**}]}]
no t1 *channel* **span** {**minor-warn** | **remove** | **major-warn**} [{**duration** *seconds* | **lcv** *threshold* [**pcv** *threshold*] [{**set** | **clear**}]}]

Syntax Description

channel	Number that indicates the T1 channel. The range is from 1 to 28.
minor-warn	Enables minor warning messages for noisy T1 links.
major-warn	Enables major warning messages for noisy T1 links.
remove	Enables removal of noisy T1 links from a multilink bundle.
lcv *threshold*	Specifies the line code violation (LCV) threshold value in bit error per second. The valid range on a T1 link is 5 to 1544 seconds. The valid range on an E1 link is 7 to 2048 seconds. • The default LCV value for minor-warn on a T1 link is 154 seconds and on E1 link is 205 seconds. • The default LCV value for major-warn or removal on a TI link is 1544 seconds and on E1 link is 2048 seconds.
duration *seconds*	Specifies the number of consecutive seconds that a threshold is exceeded or improved for a condition to occur. The valid range on a T1/E1 link is 4 to 600 seconds. The default value for T1 and E1 links is 10 seconds.
pcv *threshold*	Specifies the number of timeslots in error per second. The valid range on a T1 link is 3 to 320 seconds and on an E1 link is 8 to 832 seconds. **Note** A T1 link has 24 timeslots and an E1 link has 32 timeslots. • The default path code violation (PCV) value for minor-warn on a T1 link is 145 seconds and on E1 link is 205 seconds. • The default PCV value for major-warn or removal on a TI link is 320 seconds and on E1 link is 832 seconds.
set	(Optional) Specifies the set condition. Set is used as the default when no conditions are given.
clear	(Optional) Specifies the clear condition.

Command Default

Link Noise Monitoring on any T1 or E1 link is disabled by default. If enabled without specifying any thresholds, the default values are used as mentioned in the Syntax Description.

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
12.2(33)XNE	This command was introduced.

Usage Guidelines

Note the following when configuring link noise monitoring on T1 and E1 links:

- The **major-warn** and **remove** keywords cannot be used at the same time; disable one to use the other.
- If the **warn** and **remove** keywords are specified without any other options, the LCV and PCV thresholds and duration defaults are used to determine set (**set**) and clear (**clear**) conditions.
- If the **span** command is issued with the **set** keyword and the command is not issued again with the **clear** keyword, or vice versa, the values configured for the threshold and duration is used for both keywords.
- If the **span** command is issued without the **set** or **clear** keywords specified, **set** is the default keyword.
- The **set** and **clear** keywords can be specified only if the threshold values for the LCV and/or duration is specified.
- The threshold for a clear condition must be less than the threshold for a set condition.
- The threshold for a warn event must be less than the threshold for a remove event.
- The duration is calculated in seconds and is the number of consecutive seconds by which either of the thresholds (exceed or improve) must be surpassed for a condition to occur.
- For events, the BER on a line should be greater than or equal to (>=) the thresholds for exceed condition. For improve condition, BER has to be less than (<) the threshold.
- If the PCV threshold is not configured (using the **pcv** keyword and value), this threshold is calculated by the linear extrapolation of the Gaussian probability that is representative of most noise environments based on the configured LCV threshold. If the LCV threshold is specified, it is not mandatory to specify the PCV threshold.

Examples

The following example shows how to generate an exceed event for a minor warning, if the number of LCVs on the T1 line remain above or equal to 20, or the number of PCVs remains above or equal to 10 for 10 continuous seconds.

```
Router(config-controller)# t1 1 span minor-warn lcv 20 pcv 10 duration 10 set
```

The following example shows how to generate an improve event for a minor warning, if the number of LCVs on the T1 line remain below 15 or the number of PCVs remain below 8 for 20 continuous seconds.

```
Router(config-controller)# t1 1 span minor-warn lcv 15 pcv 8 duration 20 clear
```

The following example shows the same threshold value being used by the **set** and **clear** conditions, when both keywords are not specified. In this example, the threshold value is 80 for both conditions.

```
Router(config-controller)# t1 1 span major-warn lcv 150 pcv 100 duration 80
Router(config-controller)# end
Router# show running-config | section controller sonet 7/0/0
controller SONET 7/0/0
```

```
 framing SONET
 path 1 controller t3
 clock source internal
controller T3 7/0/0.1
 t1 1 channel-group 0 timeslots 1-24
 t1 1 span minor-warn lcv 150 pcv 100 duration 80 set
t1 1 span minor-warn lcv 150 pcv 100 duration 80 clear
```

The following example shows how the threshold value specified for the clear condition is used by the set condition when set condition is not specified. In this example, the threshold value of 100 specified for the clear condition is used for the set condition.

```
Router(config-controller)# t1 1 span major-warn lcv 100 pcv 70 duration 100 clear
Router(config-controller)# end
Router# show running-config | section controller sonet 7/0/0
controller SONET 7/0/0
 framing SONET
 path 1 controller t3
 clock source internal
controller T3 7/0/0.1
t1 1 channel-group 0 timeslots 1-24
 t1 1 span minor-warn lcv 100 pcv 70 duration 100 set
 t1 1 span minor-warn lcv 100 pcv 70 duration 100 clear
```

The following is a sample output showing the details of the calculated PCV threshold value. The calculated PCV value is 141:

```
Router# debug c10k lnm
Router(config-controller)# t1 1 span major-warn lcv 150
Router(config-controller)# end
*Sep 10 20:34:43.923:  T1 extrapolation: pcv_delta=130 lcv_delta=139 factor=140 pcv_const=14

 computed pcv_threshold = 141
*Sep 10 20:34:43.923: CMD for minor-warn set
*Sep 10 20:34:43.923: clear taking set thresholds
*Sep 10 20:34:43.923: T3 7/0/0.1#1 setting values to be sent to LC for WARN ENABLE 3
*Sep 10 20:34:43.923:
 3, 150, 150, 141, 141, 10, 10, 0, 0, 0, 0, 0, 0
Router# show running-config | section controller sonet 7/0/0
controller SONET 7/0/0
 framing SONET
 path 1 controller t3
 clock source internal
controller T3 7/0/0.1
 t1 1 channel-group 0 timeslots 1-24
 t1 1 span minor-warn lcv 150 pcv 141 duration 10 set
 t1 1 span minor-warn lcv 150 pcv 141 duration 10 clear
```

Related Commands

Command	Description
t1 clock source	Specifies where the clock source is obtained for use by each T1 channel on the channelized T3 interface.
show controllers t3	Displays the hardware and software driver information for a T3 controller.
t1 span syslog	Generates syslog messages for spans that are enabled with the link noise monitoring feature.

t1 span syslog

To generate syslog messages for all the spans on which the link noise monitoring feature is enabled, use the **t1spansyslog**command in controller configuration mode. To disable the generation of syslog messages, use the **no** form of this command.

t1 *channel* **span syslog**
no t1 *channel* **span syslog**

Syntax Description

channel	Number that indicates the T1 channel. The range is from 1 to 28.
syslog	Generates syslog messages for T1 links that are enabled with the Link Noise Monitoring feature.

Command Default

Syslog messages are disabled by default.

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
12.2(33)XNE	This command was introduced.

Usage Guidelines

The Cisco 10000 series router is a scalable platform and supports up to 4000 T1 links on one chassis. When enabled, syslog messages are generated for all T1 links on which link noise monitoring is configured. A syslog event is reported as a message. The syslog report stores the last five events.

When an ‘exceed’ event is reported, a syslog message is generated. Such syslog messages from all links clog up the logging buffer. When enabling syslog messages, a message prompts you to confirm whether to generate syslog messages or not.

To view the events for a line card, use the **showcontroller***typenumber***lnmevent**command in the privileged EXEC mode. To view the events for a SPA, use the **showplatformspa***slot/subslot***lnmevent**command.

Examples

The following example shows the message displayed when the minor warning threshold has exceeded:

```
LNM-3- MINWARNEXCEED: Interface Serial7/0/0.1/1:0, noise exceeded above minor warning
threshold
```

The following example shows the sample output of the **showcontroller** command, when executed for a specified T1 channel:

```
Router# show controllers t3 7/0/0.1 /5 lnm

Channel    Monitoring type                Thresholds (lcv/pcv/duration)
--------------------------------------------------------------------------------
  5     minor-warn (syslog disabled)   Set(154 /145 /10  ) Clear(154 /145 /10  )
Router#
```

The following example shows the sample output of the last five stored messages:

```
Router# show controller t3 7/0/0.1 lnm events
Channel          Last five events
```

```
--------------------------------------------------------------------------------
 1     MINWARNEXCEED : Noise exceeded minor-warn thresholds at Jun 11 1995 13:42:01
        MAJWARNEXCEED : Noise exceeded major-warn thresholds at Jun 11 1995 13:42:01
     MINWARNIMPROVE: Noise improved minor-warn thresholds at Jun 11 1995 13:42:01
        MAJWARNIMPROVE: Noise improved major-warn thresholds at Jun 11 1995 13:42:01
 2      Channel not configured for E1/T1
 3     Channel not configured for E1/T1
 4     No events
 5       Channel not configured for E1/T1
```

Related Commands

Command	Description
t1 clock source	Specifies where the clock source is obtained for use by each T1 channel on the channelized T3 interface.
show controllers t3	Displays the hardware and software driver information for a T3 controller.
t1 span	Enables link noise monitoring on T1 links.

t1 test

To break out a T1 channel on the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers to the test port for testing, use the **t1test**command in controller configuration mode. To remove the T1 channel from the test port, use the **no** form of this command.

t1 test *channel* [**cablelength** *feet*] [**linecode** [{**ami** | **b8zs**}]]
no t1 test *channel*

Syntax Description

channel	Number between 1 and 28 that indicates the T1 channel.
cablelength *feet*	(Optional) Specifies the cable length, in feet, from the T1 channel to the external CSU or Multi-Channel Interface Processor (MIP). Values are from 0 to 655. Default is 133.
linecode {**ami** | **b8zs**	(Optional) Specifies the line coding format used by the T1 channel. Values are alternate mark inversion (AMI) or bipolar 8 zero suppression (B8ZS). Default is B8ZS.

Command Default

No test port is configured. The default cable length is 133 feet. The default line coding is B8ZS.

Command Modes

Controller configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can use the T1 test port available on the CT3IP to break out any of the 28 T1 channels for testing (for example, 24-hour bit error-rate tester (BERT) testing as is commonly done by telephone companies before a line is brought into service).

The T1 test port is also available as an external port. For more information on configuring an external port, see the **t1external**controller configuration command.

To determine if the external device connected to the T1 test port is configured and cabled correctly before configuring a test port, use the **showcontrollerst3** command and locate the line Ext1... in the display output. The line status can be one of the following:

- LOS--Loss of signal indicates that the port is not receiving a valid signal. This is the expected state if nothing is connected to the port.
- AIS--Alarm indication signal indicates that the port is receiving an all-ones signal.
- OK--A valid signal is being received and the signal is not an all-ones signal.

Note T1 channels on the CT3IP are numbered 1 to 28 rather than the more traditional zero-based scheme (0 to 27) used with other Cisco products. This numbering scheme ensures consistency with telco numbering schemes for T1 channels within channelized T3 equipment.

Note Although you can specify a cable length from 0 to 655 feet, the hardware only recognizes the following ranges: 0 to 133, 134 to 266, 267 to 399, 400 to 533, and 534 to 655. For example, entering 150 feet uses the 134 to 266 range. If you later change the cable length to 200 feet, there is no change because 200 is within the 134 to 266 range. However, if you change the cable length to 399, the 267 to 399 range is used. The actual number you enter is stored in the configuration file.

Examples

The following example shows how to configure T1 6 on the CT3IP as a test port using the default cable length and line coding:

```
Router(config
)
# controller t3 9/0/0
Router(config
-controller)
# t1 test 6
```

Related Commands

Command	Description
show controllers t3	Displays the hardware and software driver information for a T3 controller.
t1 external	Specifies that a T1 channel on the CT3IP in Cisco 7500 series routers is used as an external port so the T1 channel can be further multiplexed on the MIP or other multiplexing equipment.

t1 timeslot

To specify the time slots and data rate used on each T1 channel on the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers, use the **t1timeslot**command in controller configuration mode. To remove the configured T1 channel, use the **no** form of this command.

t1 *channel* **timeslot** *range* [**speed** {**56** | **64**}]
no t1 *channel* **timeslot**

Syntax Description

channel	Number between 1 and 28 that indicates the T1 channel.
range	Specifies the time slots assigned to the T1 channel. The range can be from 1 to 24. A dash represents a range of time slots, and a comma separates time slots. For example, 1-10,15-18 assigns time slots 1 through 10 and 15 through 18.
speed {**56** | **64**}	(Optional) Specifies the data rate for the T1 channel, in kbps. Values are 56 or 64. The default is 64. The 56-kbps speed is valid only for T1 channels 21 through 28.

Command Default

No time slots are specified for the T1 channel. The default data rate is 64 kbps.

Command Modes

Controller configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You must specify the time slots used by each T1 channel.

Note T1 channels on the CT3IP are numbered 1 to 28 rather than the more traditional zero-based scheme (0 to 27) used with other Cisco products. This numbering scheme ensures consistency with telco numbering schemes for T1 channels within channelized T3 equipment.

Examples

The following example shows how to assign time slots 1 through 24 to T1 1 for full T1 bandwidth usage:

```
Router(config
)
# controller t3 9/0/0
Router(config
-controller)
# t1 1 timeslot 1-24
```

The following example shows how to assign time slots 21 to 23 and 26 to 28 and a data rate of 56 kbps to T1 6 for fractional T1 bandwidth usage:

```
Router(config
)
# controller t3 9/0/0
Router(config
-controller)
# t1 6 timeslot 21-23,26-28 speed 56
```

t1 yellow

To enable detection and generation of yellow alarms for a T1 channel on the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers, use the **t1yellow**command in controller configuration mode. To disable the detection and generation of yellow alarms, use the **no** form of this command.

t1 *channel* **yellow** {**detection** | **generation**}
no t1 *channel* **yellow** {**detection** | **generation**}

Syntax Description

channel	Number between 1 and 28 that indicates the T1 channel.
detection	Detects yellow alarms. This is the default, along with **generation**.
generation	Generates yellow alarms. This is the default, along with **detection**.

Command Default

Yellow alarms are detected and generated on the T1 channel.

Command Modes

Controller configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If the T1 framing type is super frame (SF), you should consider disabling yellow alarm detection because the yellow alarm can be incorrectly detected with SF framing.

Note T1 channels on the CT3IP are numbered 1 to 28 rather than the more traditional zero-based scheme (0 to 27) used with other Cisco products. This numbering scheme ensures consistency with Telco numbering schemes for T1 channels within channelized T3 equipment.

Examples

The following example shows how to disable the yellow alarm detection on T1 channel 6 on the CT3IP:

```
Router(config
)
# controller t3 9/0/0
Router(config
-controller)
# t1 6 framing sf
Router(config
-controller)
# no t1 6 yellow detection
```

tcam priority

To prioritize the interfaces for forwarding to software in the event of Ternary Content Addressable Memory (TCAM) entry or label exhaustion, use the **tcampriority** command interface configuration mode. To revert to the default setting, use the **no** form of this command.

tcam priority [{**high** | **low**}]
no tcam priority

Syntax Description

high	Sets priority to high.
low	Sets priority to low.

Command Default

normal

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The interfaces are chosen in the following order:

1. Low-priority interfaces without Vlan Access Control Lists (VACLs) and without multicast
2. Low-priority interfaces without VACLs and approved by multicast
3. Low-priority interfaces with VACLs and approved by multicast
4. Low-priority interfaces (not approved by multicast)
5. Normal-priority interfaces without VACLs and without multicast
6. Normal-priority interfaces without VACLs and approved by multicast
7. Normal-priority interfaces with VACLs and approved by multicast
8. Normal-priority interfaces (not approved by multicast)
9. High-priority interfaces without VACLs and without multicast
10. High-priority interfaces without VACLs and approved by multicast
11. High-priority interfaces with VACLs and approved by multicast
12. High-priority interfaces (not approved by multicast)

Examples

The following example shows how to set the priority to low:

```
Router(config-if)# tcam priority low
```

Related Commands

Command	Description
show tcam interface	Displays information about the interface-based TCAM.

termination

To configure the termination mode of the controller, use the **termination** command in the controller configuration mode.

termination [{**co** | **cpe**}]

Syntax Description

co	Set the line termination for the interface as CO (network)
cpe	Termination cpe (customer)

Command Default

The command default termination mode is CPE.

Command Modes

Controller configuration mode (config-controller)

Command History

Release	Modification
15.1(2)SNG	This command was implemented on Cisco ASR 901 Series Aggregation Services Routers.
15.1(2)SNG	This command was implemented on Cisco ASR 901 Series Aggregation Services Routers.

Examples

The following example shows the line termination set to "co":

```
Router(config-controller)# termination
 co
```

Related Commands

Command	Description
controller shdsl	Configures a controller for single-pair high-bit-rate digital subscriber line (SHDSL) mode.
controller shdsl	Configures a controller for single-pair high-bit-rate digital subscriber line (SHDSL) mode.

test aim eeprom

To test the data compression Advanced Interface Module (AIM) after it is installed in the Cisco 2600 series router, use the **testaimeeprom**command in privileged EXEC mode.

test aim eeprom

Syntax Description

This command has no arguments or keywords.

Command Default

No tests are performed on the data compression AIM card.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command does not have a **no** form.

Caution Using this command can erase all locations in EEPROM memory.

This command is the AIM counterpart of the **testpaseeprom** command, which performs similar tasks for port modules.

The table below shows the questions asked of the user when the **testaimeeprom** command is entered, and the recommended user responses.

Table 285: Questions and Responses for test aim eeprom Command

Questions	Responses
AIM Slot [0]:	User responds by entering the slot number of the AIM whose EEPROM is to be modified. If the user presses ENTER, the default slot 0 is used.
Use NMC93C46 ID EEPROM [y]:	User responds with “y” if the AIM contains an NMC93C46 type EEPROM and “n” if the AIM contains an X2444 EEPROM. The compression Advanced Interface Module (CAIM) contains a NMC93C46 EEPROM, and this is the default if the user just pressed ENTER.
AIM Slot %d eeprom (? for help)[%c]	General command prompt for the **testaimeeprom** command dialog. The AIM slot number chosen is displayed, and the default command is the last command entered.

Questions	Responses
Address within slot %d eeprom, [0x%02x]	Enter the desired address within the EEPROM to modify. The default is the next address beyond the byte last modified. If the user wishes to enter a hexadecimal number, it must be preceded by “0x”.
Read or Write access to slot %d at 0x%02x [%c]?	Respond with a W to write to the addressed byte or with an R to read from the addressed byte. The default value is selected by just pressing Enter and is the same as the value specified in the last primitive access.
Write data (hex 8 bits) [%02x]?:	If you respond to prompt B with “W”, then prompt C is issued, requesting the user to enter the data to write to the addressed byte. The user enters the desired value. Note that if the user desires to enter a hex value, the hex value entered must be preceded by “0x”. Otherwise, the value entered is assumed to be in decimal radix.

There is a danger that you can erase all bytes in the entire EEPROM. Though it is good to have a diagnostic tool that allows you to read and write data, there is a danger that lost data will make the Advanced Interface Module (AIM) card fail.

During your session with the test dialog, you have access to the following commands:

H or**h**	Displays a summary of the available commands.
d	Dump EEPROM contents--Displays the contents of the EEPROM in hex.
e	Erase EEPROM--Erases the entire EEPROM (all bytes set to 0xff).
p	Primitive access--Erases the EEPROM.
q	Exit EEPROM test--Causes the **testaimeepromp** command dialog to exit to the command line interface (CLI).
z	Zero EEPROM--Zeros the entire EEPROM.

Examples

The following example displays the **testaimeeprom** command user dialog:

```
Router# test aim eeprom
 AIM Slot [0]: 0
 Use NMC93C46 ID EEPROM [y]: y
 AIM Slot 0 eeprom (? for help)[?]:  ?
  d - dump eeprom contents
  e - erase all locations (to 1)
  p - primitive access
  q - exit eeprom test
  z - zero eeprom
  'c' rules of radix type-in and display apply.
 AIM Slot 0 eeprom (? for help)[?]:
```

test cable-diagnostics

To test the condition of 10-Gigabit Ethernet links or copper cables on 48-port 10/100/1000 BASE-T modules, use the **testcable-diagnostics**command in privileged EXEC mode.

test cable-diagnostics tdr interface *type number*

Syntax Description

tdr	Activates the TDR test for copper cables on 48-port 10/100/1000 BASE-T modules.
interface *type*	Specifies the interface type; see the "Usage Guidelines" section for valid values.
number	Module and port number.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(17a)SX	Support for this command was introduced on the Cisco 7600 series routers.
12.2(17b)SXA	This command was changed to provide support for the 4-port 10GBASE-E serial 10-Gigabit Ethernet module (WS-X6704-10GE).
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Cable diagnostics can help you detect whether your cable has connectivity problems.

The TDR test guidelines are as follows:

- TDR can test cables up to a maximum length of 115 meters.
- The TDR test is supported on Cisco 7600 series routers running Release 12.2(17a)SX and later releases on specific mdoules. See the Release Notes for Cisco IOS Release 12.2SX on the Catalyst 6500 and Cisco 7600 Supervisor Engine 720, Supervisor Engine 32, and Supervisor Engine 2 for the list of the modules that support TDR.
- The valid values for **interface***type*are **fastethernet** and **gigabitethernet**.
- Do not start the test at the same time on both ends of the cable. Starting the test at both ends of the cable at the same time can lead to false test results.
- Do not change the port configuration during any cable diagnostics test. This action may result in incorrect test results.
- The interface must be up before running the TDR test. If the port is down, the **testcable-diagnosticstdr** command is rejected and the following message is displayed:

```
Router# test cable-diagnostics tdr interface gigabitethernet2/12
```

```
% Interface Gi2/12 is administratively down
% Use 'no shutdown' to enable interface before TDR test start.
```

- If the port speed is 1000 and the link is up, do not disable the auto-MDIX feature.
- For fixed 10/100 ports, before running the TDR test, disable auto-MDIX on both sides of the cable. Failure to do so can lead to misleading results.
- For all other conditions, you must disable the auto-MDIX feature on both ends of the cable (use the **nomdixauto**command). Failure to disable auto-MDIX will interfere with the TDR test and generate false results.
- If a link partner has auto-MDIX enabled, this action will interfere with the TDR-cable diagnostics test and test results will be misleading. The workaround is to disable auto-MDIX on the link partner.
- If you change the port speed from 1000 to 10/100, enter the **nomdixauto**command before running the TDR test. Note that entering the **speed1000** command enables auto-MDIX regardless of whether the **nomdixauto**command has been run.

Examples

This example shows how to run the TDR-cable diagnostics:

```
Router # test cable-diagnostics tdr interface gigabitethernet2/1
TDR test started on interface Gi2/1
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

Related Commands

Command	Description
clear cable-diagnostics tdr	Clears a specific interface or clears all interfaces that support TDR.
show cable-diagnostics tdr	Displays the test results for the TDR cable diagnostics.

test interface fastethernet

To test the Fast Ethernet interface by causing the interface to ping itself, use the **testinterfacefastethernet** command in user EXEC or privileged EXEC mode.

test interface fastethernet *number*

Syntax Description

number	Port, connector, or interface card number. On a Cisco 4500 or Cisco 4700 series router, specifies the network processor module (NPM) number. The numbers are assigned at the factory at the time of installation or when added to a system and are displayed with the **showinterfaces** command.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command sends pings from the specified interface to itself. Unlike the **ping** command, the **testinterfacefastethernet** command does not require the use of an IP address.

Examples

The following example shows how to test a Fast Ethernet interface on a Cisco 4500 router:

```
Router# test interface fastethernet 0
```

Related Commands

Command	Description
ping (privileged)	Diagnoses basic network connectivity on AppleTalk, CLNS, DECnet, IP, or Novell IPX networks.
ping (user)	Provides simple ping diagnostics of network connectivity.
show interfaces	Displays information about interfaces.

test platform police get

To get the IPv6 internal police rate, use the *test platform police get* command in privileged EXEC mode.

test platform police get

Syntax Description

This command has no arguments or keywords.

Command Default

0 (No rate has been applied.)

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRD1	The command was introduced on the Cisco 7600 series routers for the ES+ line cards, the SIP-400, and the 7600-ES+ITU-2TG and 7600-ES+ITU-4TG.

Usage Guidelines

Use this command under the exec command of the line card console. It is not visible from the route processor (RP) console.

Examples

The following example shows how to get the IPv6 internal police rate:

```
Router> enable
Router# test platform police get
IPv6 with HBH header is policed at 100000 kbps
```

Related Commands

Command	Description
test platform police set	Sets the IPv6 internal police rate.

test platform debugger rommon

To configure the ROM monitor (ROMMON) variables on a Route Processor (RP) or a Switch Processor (SP), use the **test platform debugger rommon** command in privileged EXEC mode.

test platform debugger rommon[{**dump** | **get** *string* | **set** *string* | **unset** *string*}]

Syntax Description

dump	Displays all configured ROMMON variables.
get	Reads the specified ROMMON variable.
set	Modifies the specified ROMMON variable.
unset	Unsets the specified ROMMON variable.
string	Name of the specified ROMMON variable.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(4)S	This command was introduced.

Usage Guidelines

This command is supported on both Route Switch Processor (RSP) and Supervisor Engine (SUP), but works only on the RSP.

Examples

This example shows how to configure a ROMMON variable:

```
Router# test platform debugger rommon dump
Router# test platform debugger rommon unset string
Router# test platform debugger rommon get string
Router# test platform debugger rommon set string
```

test platform police ipv6 disable

To disable the IPv6 internal policer, use the **test platform police ipv6 disable** command in privileged EXEC mode.

test platform police ipv6 disable

Syntax Description

This command has no arguments or keywords.

Command Default

0 (No rate has been applied)

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)S1	The command was introduced on the Cisco 7600 series routers for the ES+ line cards, the SIP-400, and the 7600-ES+ITU-2TG and 7600-ES+ITU-4TG.

Usage Guidelines

Use this command under the **exec** command of the line card console. It is not visible from the route processor (RP) console.

Examples

This example shows how to disable the IPv6 internal police rate:

```
Router(config)#test platform police ipv6 disable
```

Related Commands

Command	Description
test platform police ipv6 set	Sets the IPv6 internal police rate.
test platform police ipv6 get	Gets the IPv6 internal police rate.

test platform police set

To set the IPv6 internal police rate, use the *test platform police set* command in privileged EXEC mode. This command does not have a no form.

If you have set a rate limit and wish to cancel it, you will need to use this command to set the rate to 0.

test platform police set rate

Syntax Description

rate	Specifies the internal police rate. The range is from 0 to 100000 kbps.
	• For the SIP-400, you can configure a rate up to, and including 25600 packets per second (PPS).
	• For the ES+ line cards and the 7600-ES+ITU-2TG and 7600-ES+ITU-4TG line cards, you can configure rates of:
	  • 16 Kbps to 2 Mbps; granularity of 16 kbps
	  • 2 Mbps to 100 Mbps; granularity of 64 kbps

Command Default

For ES40 line cards, the default police rate is 12.8 Mbps.

For the SIP-400, the default police rate is 21.36 kpps.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRD1	The command was introduced on the Cisco 7600 series routers for the ES+ line cards, the SIP-400, and the 7600-ES+ITU-2TG and 7600-ES+ITU-4TG.

Usage Guidelines

Use this command under the EXEC command of the line card console. It is not visible from the route processor (RP) console.

For both the ES+ line cards and the SIP-400, setting the police rate to 0 turns off the policing.

For both the ES+ line cards and the SIP-400, when the policer is set from the the line card console, the setting remains effective even if the line card is moved to another chassis running the Cisco IOS Release 12.2(33)SRD1 (or later) image.

For the SIP-400, IPv6 HBH packets will continue to go through the QoS policing configured on the line card. For ES+ line cards, IPv6 HBH packets will bypass any QoS configured on the line card.

Examples

The following examples shows how to set the IPv6 with HBH header to be policed at 100000 kbps:

```
Router> enable
Router# test platform police set 100000
```

Related Commands

Command	Description
test platform police get	Gets the IPv6 internal police rate.

test satellite satellite mfg link

To force the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT) to show that the backbone link to the hub is up, even when the link is actually down, use the **testsatellitesatellitemfglink** command in privileged EXEC mode.

test satellite satellite *slot/unit* **mfg link** {**force** | **normal**}

Syntax Description

slot	Router chassis slot in which the network module is installed.
unit	Interface number. For NM-1VSAT-GILAT network modules, always use 0.
force	Forces the satellite link to appear to be UP.
normal	Allows the satellite link to display the actual status, UP or DOWN.

Command Default

The actual status (UP or DOWN) of the satellite link is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Use the **testsatellitesatellitemfglink**command only when instructed by your satellite service provider or a technical support representative.

Examples

The following example shows how to force the NM-1VSAT-GILAT network module to show that the backbone link to the hub is up, even if the link is actually down:

```
Router# test satellite satellite 1/0 mfg link force
```

The following example shows how to allow the NM-1VSAT-GILAT network module to show the actual status (UP or DOWN) of the satellite link:

```
Router# test satellite satellite 1/0 mfg link normal
```

test satellite satellite reset

To reset the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT), use the **testsatellitesatellitereset** command in privileged EXEC mode.

test satellite satellite *slot/unit* **reset** [**hard**]

Syntax Description

slot	Router chassis slot in which the network module is installed.
unit	Interface number. For NM-1VSAT-GILAT network modules, always use 0.
hard	Hardware reset. Not available on all routers.

Command Default

Without the **hard** keyword, the command initiates a software reset.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Use the **testsatellitesatellitereset** command only when instructed by your satellite service provider or a technical support representative. You will lose satellite network connectivity while the NM-1VSAT-GILAT network module resets.

We recommend that you first try a software reset. The hardware reset option is not available on all routers.

Examples

The following example shows how to initiate a software reset of the NM-1VSAT-GILAT network module:

```
Router# test satellite satellite 1/0 reset
```

The following example shows how to initiate a hardware reset of the NM-1VSAT-GILAT network module:

```
Router# test satellite satellite 1/0 reset hard
```

test service-module

To perform self-tests on an integrated CSU/DSU serial interface module, such as a 4-wire, 56/64 kbps CSU/DSU, use the **testservice-module** command in privileged EXEC mode.

test service-module commandtest service-module *interface-type interface-number*

Syntax Description

interface-type	Interface type.
interface-number	Interface number.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The following tests are performed on the CSU/DSU:

- ROM checksum test
- RAM test
- EEPROM checksum test
- Flash checksum test
- DTE loopback with an internal pattern test

These self-tests are also performed at power on.

This command cannot be used if a DTE loopback, line loopback, or remote loopback is in progress.

Data transmission is interrupted for 5 seconds when you issue this command. To view the output of the most recent self-tests, use the**showservice-module**command.

This command does not have a **no** form.

Examples

The following example shows how to perform a self-test on serial interface 0:

```
Router# test service-module serial 0
SERVICE_MODULE(0): Performing service-module self test
SERVICE_MODULE(0): self test finished: Passed
```

Related Commands

Command	Description
channelized	Clears the interface counters.
clear service-module serial	Resets an integrated CSU/DSU.
show service-module serial	Displays the performance report for an integrated CSU/DSU.

test trunk

To configure the test port on a trunk card, use the **testtrunk** command in privileged EXEC mode.

test trunk stm1 {**drop** | **monitor**} {**tx** | **rx**} {**on** | **off**} **e1** *controller*

Syntax Description

stm1	Specifies the test port on an STM-1 trunk card. This keyword is supported only on the Cisco AS5850 platform.
drop	Specifies drop mode where the existing signal is dropped and the signal from the test port is sent to the controller.
monitor	Specifies monitor mode where the signal from the specified E1 controller is monitored via the test port. The original signal is not disturbed.
tx	Specifies that signal is sent on the transmit line.
rx	Specifies that signal is sent on the receive line.
on	Switches the test port on.
off	Switches the test port off.
e1	Specifies that an E1 controller is to be used for testing.
controller	Slot and port numbers to identify the E1 controller.

Command Default

The test port is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(15)T	The **stm-1** keyword was added.

Usage Guidelines

If a controller does not go up, or there are a large number of errors associated with a specific E1 controller, you might be able to determine whether the problem is in the server card or in an external line by using the test port. The test port is located on the front panel of the SDH/STM-1 trunk card.

This command does not have a **no** form because the command itself switches the test port on or off.

To use this command, one E1 controller is selected and the transmit and receive lines can be put into drop or monitor mode. Both drop and monitor modes can be used at the same time on either the transmit or receive lines, but both transmit and receive lines cannot be used in drop or monitor mode at the same time.

Examples

The following example shows how to configure a test port to use drop mode on the receive line of an E1 controller in the second path of an STM-1 trunk card in slot 2 of a Cisco AS5850 chassis:

```
Router# test trunk stm-1 drop rx on E1 2/0.2/1/2
```

threshold

To set the path BER threshold values, configure the **threshold** command in the controller configuration mode. To return to the default value, use the no form of this command.

threshold { *b1-tca* | *b2-tca* | *b3-tca* | *sd-ber* | *sf-ber* *bit-error-rate*

Syntax Description

b1-tca	Enables Bit Error Rate (BER) threshold crossing alerts for B1.
b2-tca	Enables BER threshold crossing alerts for B2.
b3-tca	Enables BER threshold crossing alerts for B3. Configures path threshold.
sd-ber	Enables the threshold of the Signal Degrade (SD) BER that is used to trigger a signal degrade alarm.
sf-ber	Configures the threshold of the Signal Failure (SF) BER that is used to trigger a link state change.
bit-error-rate	Specifies the BER.

Command Default

None

Command Modes

Controller configuration

Command History

Release	Modification
XE 3.18 SP	Support for this command was introduced on NCS 4200 Series.

Usage Guidelines

This command is used to configure line, section, and path threshold.

Examples

The following example shows the configuration of line and section threshold:

```
enable
configure terminal
controller MediaType 0/5/0
mode sonet
controller sonet 0/5/0
sts-1 1
threshold b3-tca 3
end
```

Related Commands

Command	Description
controller sonet	Configures the SONET mode.
show controller sonet	Displays SONET controller configuration.

timeslot

To enable framed mode on a serial interface on a G.703 E1 port adapter, an FSIP, or an E1-G.703/G.704 serial port adapter, use the **timeslot** command in interface configuration mode. To restore the interface to unframed mode, use the **no** form of this command or set the start slot to 0.

timeslot *start-slot* *stop-slot*
no timeslot

Syntax Description

start-slot	First subframe in the major frame. Valid range is from 1 to 31 and must be less than or equal to the *stop-slot*value.
stop-slot	Last subframe in the major frame. Valid range is from 1 to 31 and must be greater than or equal to the *start-slot*value.

Command Default

The default G.703 E1 interface is not configured for framed mode.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
11.1 CA	This command was modified to include the E1-G.703/G.704 serial port adapter and Cisco 7200 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Framed mode allows you to specify a bandwidth for the interface by designating some of the 32 time slots for data and reserving the others for framing (timing). Unframed mode, also known as clear channel, does not reserve any time slots for framing.

This command applies to Cisco 4000, 7000, 7200, and 7500 series routers. G.703 E1 interfaces have two modes of operation, framed and unframed. When in framed mode, the range from *start-slot* to *stop-slot* gives the number of 64-kbps slots in use. There are thirty-two 64-kbps slots available.

In framed mode, timeslot 16 is not used for data. To use timeslot 16 for data, use the **ts16** interface configuration command.

Examples

The following example shows how to enable framed mode on a serial interface on a G.703 E1 port adapter or an E1-G.703/G.704 port adapter:

```
Router(config
)
# interface serial 3/0
Router(config
```

```
-if)
# timeslot 1-3
```

Related Commands

Command	Description
ts16	Controls the use of timeslot 16 for data on a G.703 E1 interface or on an E1-G703/G.704 serial port adapter.

time-properties persist

To configure the time-properties holdover time, use the **time-properties persist** command in PTP clock configuration mode.

time-properties persist *value*

Syntax Description

value	Time-properties holdover time. Valid values are from 0 to 10000 seconds. The default value is 300 seconds.

Command Default

By default holdover time is 300 seconds.

Command Modes

PTP clock configuration (config-ptp-clk)

Command History

Release	Modification
Cisco IOS XE 3.18.1SP	This command was introduced.

Usage Guidelines

When a master clock is lost, the time properties holdover timer starts. During this period, the time properties flags (currentUtcOffset, currentUtcOffsetValid, leap61, leap59) persist for the holdover timeout period. Once the holdover timer expires, currentUtcOffsetValid, leap59, and leap61 flags are set to false and the currentUtcOffset remains unchanged.

The following example shows how to configure the current UTC offset, leap second event date and offset value:

```
Device(config)# ptp clock boundary domain 0 hybrid
Router(config-ptp-clk)# time-properties persist 600
Router(config-ptp-clk)#utc-offset 45 leap-second "01-01-2017 00:00:00" offset 1
```

Related Commands

Command	Description
utc-offset leap-second offset	Configures the current UTC offset, leap second event date and Offset value (+1 or -1).

tod

To configure the time of day message format used by the 1PPS interface, use the **tod** command in PTP clock port configuration mode. To remove a time of day configuration, use the **no** form of this command.

tod *slot/bay* {**iso8601** | **ubx** | **nmea** | **cisco** | **ntp**} [**delay** *delay-amount*]
no tod *slot/bay* {**iso8601** | **ubx** | **nmea** | **cisco** | **ntp**} [**delay** *delay-amount*]

Syntax Description

slot	Slot of the 1PPS interface.
bay	Bay of the 1PPS interface.
iso8601	Specifies ISO 8601 time of day format.
ubx	Specifies UBX time of day format.
nmea	Specifies NMEA time of day format.
cisco	Specifies Cisco time of day format.
ntp	Specifies NTP time of day format.
delay	(Optional) Specifies a delay between the 1PPS message and the time of day message.
delay-amount	Amount of delay between the 1PPS message and the time of day message, in milliseconds. The range is from 1 to 999.

Command Default

The time of day message format is not configured.

Command Modes

PTP clock port configuration (config-ptp-clk)

Command History

Release	Modification
15.0(1)S	This command was introduced.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

This command applies only to platforms that have 1PPS ports.

Examples

The following example shows how to configure a time of day value:

```
Device> enable
Device# configure terminal
Device(config)# ptp clock ordinary domain 0
Device(config-ptp-clk)# tod 3/0 ntp
Device(config-ptp-clk)# end
```

This example sows the configuration of the time of (ToD) message format for a 1588V2 primary on a Cisco ASR 901 Series Aggregation Services Router:

```
Device> enable
Device# configure terminal
Device(config)# ptp clock ordinary domain 0
Device(config-ptp-clk)# tod 3/0 cisco
Device(config-ptp-clk)# input 1pps 3/3
Device(config-ptp-clk))# clock-port MASTER master
Device(config-ptp-clk)# transport ipv4 unicast interface Gi3/3/1 negotiation
Device(config-ptp-clk)# end
```

Related Commands

Command	Description
input	Enables PTP input clocking using the 1.544 Mhz, 2.048 Mhz, or 10 Mhz timing interface or phase using the 1PPS or RS-422 interface.
output	Enables output of time of day messages using the 1PPS interface.

transceiver type all

To enable the monitoring of all transceivers via the transceiver type configuration mode, use the **transceivertypeall** command in global configuration mode. This command does not have the **no** form.

transceiver type all

Syntax Description

This command has no arguments or keywords.

Command Default

Transceiver type configuration is disabled. If transceiver type configuration is enabled, the default monitoring interval is 600 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.2(33)SXH	This command was modified. The **interval** keyword was removed.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.2(2)SNI	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

You can enter the transceiver type configuration mode using the **transceiver type all** command. You can then monitor the transceiver types and also set the monitoring interval using the **monitoring** command.

Examples

This example shows how to enter in to transceiver type configuration mode and then enable the monitoring for all transceiver types:

```
Router(config)# transceiver type all
Router(config-xcvr-type)# monitoring interval 500
```

Related Commands

Command	Description
monitoring	Enables to monitor the transceiver types and also set the monitoring interval.
snmp-server enable traps transceiver type all	Enables all supported SNMP transceiver traps for all transceiver types.

transmit-buffers backing-store

To buffer short-term traffic bursts that exceed the bandwidth of the output interface, use the **transmit-buffersbacking-store**command in interface configuration mode. To disable this function, use the **no** form of this command.

transmit-buffers backing-store
no transmit-buffers backing-store

Syntax Description

This command has no arguments or keywords.

Command Default

The default is off, unless weighted fair queueing is enabled on the interface. If weighted fair queueing is enabled on the interface, the **transmit-buffersbacking-store** command is enabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced on the Cisco 7500 series router.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If the **transmit-buffersbacking-store** command is enabled and a full hardware transmit queue is encountered, packets are swapped out of the original memory device (MEMD) into a system buffer in DRAM. If the **transmit-buffersbacking-store** command is not enabled and the output hold queue is full, packets are dropped instead of being copied if a full hardware transmit queue is encountered. In both cases, the original MEMD buffer is freed so that it can be reused for other input packets.

To preserve packet order, the router checks the output hold queue and outputs previously queued packets first.

Examples

The following example shows how to enable the **transmit-buffersbacking-store** command on a FDDI interface:

```
Router(config
)
# interface fddi 3/0
Router(config
-if)
# transmit-buffers backing-store
```

Related Commands

Command	Description
fair-queue (WFQ)	Enables WFQ for an interface.

transmit-clock-internal

To enable the internally generated clock on a serial interface on a Cisco 7200 series or Cisco 7500 series router when a DTE does not return a transmit clock, use the**transmit-clock-internal** command in interface configuration mode. To disable the internally generated clock, use the **no** form of this command.

transmit-clock-internal
no transmit-clock-internal

Syntax Description

This command has no arguments or keywords.

Command Default

The internally generated clock is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to enable the internally generated clock on serial interface 3/0 on a Cisco 7200 series or Cisco 7500 series router:

```
Router(config
)
# interface serial 3/0
Router(config
-if)
# transmit-clock-internal
```

transmit-interface

To assign a transmit interface to a receive-only interface, use the **transmit-interface** command in interface configuration mode. To return to normal duplex Ethernet interfaces, use the **no** form of this command.

trtransmit-interface commandansmit-interface *type number*
no transmit-interface

Syntax Description

type	Transmit interface type to be linked with the (current) receive-only interface.
number	Transmit interface number to be linked with the (current) receive-only interface.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Receive-only interfaces are used commonly with microwave Ethernet links.

Examples

The following example specifies Ethernet interface 0 as a simplex Ethernet interface:

```
interface ethernet 1
 ip address 128.9.1.2
 transmit-interface ethernet 0
```

transmitter-delay

To specify a minimum dead-time after transmitting a packet, use the **transmitter-delay**command in interface configuration mode. To restore the default, use the**no**form of this command.

transmitter-delay *delay*
no transmitter-delay

Syntax Description

delay	On the FSIP, high-speed serial interface (HSSI, and) on the IGS router, the minimum number of High-Level Data Link Control (HDLC) flags to be sent between successive packets. On all other serial interfaces and routers, approximate number of microseconds of minimum delay after transmitting a packet. The valid range is from 0 to 131071. Default is 0. For all interfaces using chipset CD2430 , the default is 2.

Command Default

0 flags or microseconds 2 for all interfaces using chipset CD2430

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is especially useful for serial interfaces that can send back-to-back data packets over serial interfaces faster than some hosts can receive them.

The transmitter delay feature is implemented for the following Token Ring cards: CSC-R16, CSC-R16M, CSC-1R, CSC-2R, and CSC-CTR. For the first four cards, the command syntax is the same as the existing command and specifies the number of microseconds to delay between sending frames that are generated by the router. Transmitter delay for the CSC-CTR uses the same syntax, but specifies a relative time interval to delay between transmission of all frames.

Examples

The following example shows how to specify a delay of 300 microseconds on serial interface 0:

```
Router(config
)
# interface serial 0
Router(config
-if)
# transmitter-delay 300
```

transport-mode

To configure a transport mode, use the **transport-mode**command in interface configuration mode. To return to the default state, use the **no** form of this command.

transport-mode {**lan** | **wan** | **otn** **bit-transparent** {**opu1e** | **opu2e**}}
no **transport-mode** {**lan** | **wan** | **otn** **bit-transparent** {**opu1e** | **opu2e**}}
transport-mode otn *otu4 100G*

Syntax Description

lan	10GBASE-R LAN pass-through mode (10.3125 Gb/s)
wan	10GBASE-W WAN (SONET/SDH) mode (9.95328 Gb/s)

otn	Optical Transport Network (G.709). The following modes are supported under interface OTN:
	• bit-transparent--XAUI transparently mapped into OTU-2 (11.096 or 11.049 Gb/s)
	  • opu1e--Over OPU1e (11.0491 Gb/s)
	  • opu2e--Over OPU2e (11.0957 Gb/s)

otu4	The encapsulation type

Command Default

LAN

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SRD1	This command was introduced on the Cisco 7600 series router.

Examples

The following example shows how to configure a LAN transport mode:

```
Router(config-if)# transport-mode lan
```

Examples

The following example shows how to configure a LAN transport mode:

```
Router(config-if)# transport-mode otn otu4 100G
```

Related Commands

Command	Description
controller dwdm	Configures a DWDM controller.
g709 fec	Configures the FEC for the DWDM controller.
g709 odu threshold	Configures thresholds for selected ODU BER alarms.
g709 otu threshold	Configures thresholds for selected OTU BER alarms.

Command	Description
no g709 odu report	Disables the logging of selected ODU alarms.
no g709 otu report	Disables the logging of selected OTU alarms.
show controller dwdm	Displays ITU-T G.709 alarms, alerts, and counters.

transport ipv4

To specify IPv4 transport source mode and the transport source interface, use the **transportipv4** command in L3 VPN encapsulation configuration mode. To remove the transport source, use the **no** form of this command.

transport ipv4 [**source** *interface-type interface-number*]
no transport [**ipv4**]

Syntax Description

source	Specifies the IPv4 transport source.
interface-type	(Optional) The source interface type.
interface-number	(Optional) The source interface number.

Command Default

The IPV4 transport source mode and interface are not defined.

Command Modes

L3VPN Encapsulation Configuration (config-l3vpn-encap-ip)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.

Usage Guidelines

The **transportipv4** command specifies IPv4 transport source mode and defines the transport source interface while configuring the L3VPN encapsulation profile. When you use this command, make sure that the specified source address is used as the nexthop in BGP updates advertised by the PE.

Examples

The following example shows how to specify IPv4 transport source mode and the transport source interface:

```
Router(config-l3vpn-encap-ip)# transport ipv4 source loopback 0
```

Related Commands

Command	Description
l3vpn encapsulation ip	Configures the L3VPN encapsulation profile.
protocol gre	Specifies GRE as the tunnel mode and sets the GRE key.
show l3vpn encapsulation ip	Displays the profile health and the underlying tunnel interface.

transport ipv4 (PTP)

To specify the IP version, transmission mode, and interface that a Precision Time Protocol clock port uses to exchange timing packets, use the **transport ipv4** command in PTP clock port configuration mode. To remove a transport configuration, use the **no** form of this command.

transport ipv4 {**unicast** | **multicast** | **multicast-mix**} **interface** *interface-type interface-number* [**negotiation**]
no transport ipv4 {**unicast** | **multicast** | **multicast-mix**} **interface** *interface-type interface-number* [**negotiation**]

Syntax Description

unicast	Configures the clock port to exchange timing packets in unicast mode.
multicast	Configures the clock port to exchange timing packets in multicast mode.
multicast-mix	Configures the clock port to exchange timing packets in multicast-unicast communication mode. In multicast-unicast mode, the clock port sends initial Announce and Sync messages as multicast; if a subordinate device responds with a unicast message, the clock port sends the Delay-Resp message as unicast.
interface	Specifies an interface on the device.
interface-type	The type of the interface.
interface-number	The number of the interface.
negotiation	(Optional) Enables dynamic discovery of subordinate devices and their preferred format for sync interval and announce interval messages.

Command Default

The IP version, transmission mode, and interface are not specified for exchanging timing packets.

Command Modes

PTP clock port configuration (config-ptp-clk)

Command History

Release	Modification
15.0(1)S	This command was introduced.
15.1(2)SNG	This command was implemented on Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

You can configure different transport values for each PTP clock port.

Examples

The following example shows how to use the **transportipv4** command:

```
Device> enable
Device# configure terminal
Device(config)# ptp clock ordinary domain 0
Device(config-ptp-clk)# clock-port masterport master
Device(config-ptp-clk)# transport ipv4 unicast interface top5/2/2
Device(config-ptp-clk)# end
```

Related Commands

Command	Description
clock-port	Specifies the mode of a PTP clock port.

ts16

To control the use of time slot 16 for data on a G.703 E1 interface or on an E1-G.703/G.704 serial port adapter, use the **ts16** command in interface configuration mode. To restore the default, use the **no** form of this command.

ts16
no ts16

Syntax Description

This command has no arguments or keywords.

Command Default

Time slot 16 is used for signaling.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
11.1CA	This command was implemented on the E1-G.703/G.704 serial port adapter and Cisco 7200 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command applies to Cisco 4000, 7000, 7200, and 7500 series routers. By default, time slot 16 is used for signaling. Use this command to configure time slot 16 to be used for data. When in framed mode, in order to get all possible subframes or time slots, you must use the **ts16** command.

Examples

The following example shows how to configure time slot 16 to be used for data on a G.703 E1 interface or an E1-G.703/G.704 serial port adapter:

```
Router(config
-if)
# ts16
```

Related Commands

Command	Description
timeslot	Enables framed mode serial interface on a G.703 E1 port adapter, an FSIP, or an E1-G.703/G.704 serial port adapter.

ttb

To send a trace trail buffer in E3 g832 framing mode, use the **ttb** command in interface configuration mode. To disable the trace, use the **no** form of this command.

ttb {**country** | **rnode** | **serial** | **snode** | **soperator** | **x**} *line*
no ttb {**country** | **rnode** | **serial** | **snode** | **soperator** | **x**} *line*

Syntax Description

country *line*	Two-character country code.
rnode *line*	Receive node code.
serial *line*	M.1400 Serial
snode *line*	Sending Town/Node ID code.
soperator *line*	Sending Operator code.
x *line*	XO

Command Default

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
12.2S	This command was introduced.
12.2(25)S3	This command was integrated into Cisco IOS Release 12.2(25)S3 to support SPAs on the Cisco 7304 routers.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE to support SPAs on the Cisco 7600 series routers and Catalyst 6500 series switches.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S to support SPAs on the Cisco 12000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **ttb** command to attach a header that contains fields to send to a remote device.

Examples

The following example starts a TTB message on the first port on slot 5.

```
Router# configure terminal
Router(config)# int serial 5/0/0
Router(config-if)# ttb country us
Router(config-if)# ttb snode 123
Router(config-if)# ttb rnode rn
Router(config-if)# ttb x 9
Router(config-if)# ttb serial 432
```

Related Commands

Command	Description
show controller serial	Displays controller statistics.

ttl

Use this command to configure static pseudowire OAM class configuration .

ttl *value*

Syntax Description

Syntax Description:

value	TTL value for multi-segment pseudowire OAM data

Command Default

Default value is 1

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1	This command was introduced into the Cisco ASR 920 Routers.

Examples

The following example shows how to configure static pseudowire OAM:

```
enable
configure terminal
pseudowire-static-oam class oam-class1
timeout refresh send 20
ttl 3
end
```

tu-ais

To enable the SDH device to detect the PDH AIS alarm TU-AIS alarms are generated and detected when the TDM circuits go down on the access layer of the network topology or a failure occurs in MPLS domain due to which SAToP connectivity goes down, use the tu-ais command in SONET configuration mode. To disable the TU-AIS alarms, use the no form of this command..

tu-ais

no tu-ais

Syntax Description

Syntax Description

This command has no keywords or arguments.

Command Default

This command is disabled by default; no TU-AIS alarm is sent.

Command Modes

SONET configuration

Command History

Release	Modification
IOS XE Everest 16.6.1	Support for this command was introduced on the Cisco ASR 900 Routers.

Usage Guidelines

The TU-AIS alarms are supported on the OC3 IM in Cisco ASR 903 RSP1 and RSP2 modules according to TU-12 section as defined in ITU-G. 707 (8.3.2). TU-AIS means that all TU-12 (i.e. all 144B) carries all "1" according to ITU-T G.707 (6.2.4.1.3).

Examples

The following example shows the configuration of AIS SHUT:

```
enable
configure terminal
controller sonet 0/5/0
tu-ais
end
```

Related Commands

Command	Description
controller sonet	Configures the SONET mode.
show controller sonet	Displays SONET controller configuration.
show run | se	Displays the TU-AIS alarm configuration.

tug-2

Use this command to configure mode Tributary Unit group type 2 (TUG-2) number that has been mapped to an AU-4.

tug-2 *tug-2 number* **payload** [*VC11* | *VC12*]

Syntax Description

Syntax Description

tug-2 number	The range is from 1 to 7.
payload	Specifies VC11 or VC12 payload.
VC11	TUG-2 payload VC-11 can be configured as VC or T1 and the range is 1 to 4.
VC12	TUG-2 payload VC-12 can be configured as VC or E1 and the range is 1 to 3.

Command Default

None

Command Modes

Controller configuration

Command History

Release	Modification
XE Everest 16.6.1	This command was integrated into the Cisco NCS 4200 Series and Cisco ASR 900 Series.

Usage Guidelines

When you configure mode VC-1x, seven TUG-2 payloads are created. TUG-2 payloads can be of two types, VC-11 and VC-12. Default for TUG-2 payload mode is VC-11.

Examples

```
enable
configure terminal
controller sdh 0/5/0
rate stm4
au-4 1
mode tug-3
tug-3 1
mode vc1x
cem-group 100 unframed
end
```

Related Commands

Command	Description
show running configuration	Verifies TUG-3 configuration.

tug-2 e1

To create E1 controllers for a specified path under the Tributary Unit group type 2 (TUG-2), use the **tug-2e1**command in controller configuration mode.

tug-2 *tug-2-number* **e1** *e1-number*

Syntax Description

tug-2-number	Number, or range of numbers, from 1 to 7. To specify a range of TUG-2 numbers use a dash between the values, for example 1-5. An individual TUG-2 can be specified using a comma between values, for example 2,4. Default is 1.
e-1-number	Number, or range of numbers, from 1 to 3. To specify a range of E1 numbers use a dash between the values, for example 1-3. An individual E1 can be specified using a comma between values, for example 2,3.

Command Default

Default *tug-2-number* value for STM-1 card is 1.

Command Modes

Controller configuration

Command History

Release	Modification
12.0(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines

Use the **tug-2e1** command to create an E1 controller with the following name format:

slot/port.path/tug-2-number/e1-number

Up to 21 controllers can be created for one path. Only one path can be selected at a time.

Examples

The following example shows how to configure 15 E1 controllers on the second path of an STM-1 in physical slot number 2 of a Cisco AS5850 chassis:

```
Router(config)# controller sonet 2/0
Router(config-controller)# aug mapping au-4
Router(config-ctrlr-tug3)# au-4 1 tug-3 2
Router(config-ctrlr-tug3)# tug-2 5 e1 3
```

Related Commands

Command	Description
show controller sonet	Displays information about SONET controllers.

tug-2 e1 bert pattern

To send a BER test pattern on an E1 line that has been mapped to a TUG-3, use the **tug-2e1bertpattern**command in configuration controller tug3 mode.

To send a BER test pattern on an E1 line that has been mapped to an AU-3, use the **tug-2e1bertpattern**command in configuration controller au3 mode.

To stop the BER test, use the **no** form of this command.

tug-2 *tug-2 number* **e1** *e1-number* [**bert pattern** *pattern* **interval** *time*]
[**no**] **tug-2** *tug-2 number* **e1** *e1-number* [**bert pattern** *pattern* **interval** *time*]

Syntax Description

tug-2 number	A number in the range of 1 to 7.
e1-number	A number in the range of 1 to 3.
pattern	• 2^11, pseudorandom test pattern (2048 bits long). • 2^15, pseudorandom O.151 test pattern (32,768 bits long). • 2^20-O153, 2^20-1 O.153 test pattern. • 2^20-QRSS, pseudorandom QRSS O.151 test pattern (1,048,575 bits long).
time	An interval in the range of 1 to14,400 minutes.

Command Default

No BER test is configured.

Command Modes

Configuration controller tug3 (for an E1 line mapped to a TUG-3) Configuration controller au3 (for an E1 line mapped to an AU-3)

Command History

Release	Modification
12.0(14)S	This command was introduced.
12.1(7)E	Support for this command was integrated into Cisco IOS Release 12.1(7)E. Support for this command was added for Cisco 7200 VXR routers and Catalyst 6000 family switches.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the tug-2 e1 bert pattern command in configuration controller tug3 command mode to send a BERT test on an E1 line that has been mapped to a TUG-3 via the aug mapping au-4 command.

Use the tug-2 e1 bert pattern command in configuration controller au3 command mode to send a BERT test on an E1 line that has been mapped to an AU-3 via the aug mapping au-3 command.

To view the test results of a BER test pattern, use the show controller sonet command.

Examples

The following example sends a BER 2^11 pseudorandom pattern through E1 line 1, that has been mapped to a TUG-3 on a Cisco 7500 series router, for five minutes:

```
Router(config)# controller sonet 2/0/0
Router(config-controller)# aug mapping au-4
Router(config-controller)# au-4 1 tug-3 2
Router(config-ctrlr-tug3)# tug-2 4 e1 1 bert pattern 2^11 interval 5
```

The following example sends a BER 2^15 pseudorandom pattern through E1 line 1, that has been mapped to an AU-3 on a Cisco 7200 VXR router or a Catalyst 6000 family switch, for ten minutes:

```
Router(config)# controller sonet 2/0
Router(config-controller)# aug mapping au-3
Router(config-controller)# au-3 1
Router(config-ctrlr-au3)# tug-2 4 e1 1 bert pattern 2^15 interval 10
```

Related Commands

Command	Description
aug mapping	Configures the AUG mapping mode of the PA-MC-STM-1.
au-3	Configures a particular AU-3 of an E1 line that has been mapped to an AU-3.
au-4 tug-3	Specifies the AU-4 and TUG-3 number of an E1 line that has been mapped to an AU-4.

tug-2 e1 channel-group timeslots

To create a logical channel group on an E1 line that has been mapped to a TUG-3 or AU-3, use the **tug-2e1channel-grouptimeslots** command in the appropriate configuration mode. To remove a logical channel group, use no the form of this command.

tug-2 *tug-2-number* **e1** *e1-number* [[**channel-group** *channel-group-number*] [**timeslots** *list-of-timeslots*]]
no tug-2 *tug-2-number* **e1** *e1-number* [[**channel-group** *channel-group-number*] [**timeslots** *list-of-timeslots*]]

Syntax Description

tug-2-number	A number in the range of 1 to 7.
e1-number	A number in the range of 1 to 3.
channel-group	Defines a logical channel group to be a channelized E1 line.
channel-group-number	(Optional) A number in the range of 0 to 30.
timeslots	(Optional) Creates the time slots that make up the E1 line.
list-of-timeslots	(Optional) A number in the range of 1 to 31 or a combination of subranges within 1 to 31.

Command Default

No channel groups are configured on an E1 line.

Command Modes

Configuration controller tug3 (for an E1 line mapped to a TUG-3) Configuration controller au3 (for an E1 line mapped to an AU-3)

Command History

Release	Modification
12.0(14)S	This command was introduced.
12.1(7)E	Support for this command was integrated into Cisco IOS Release 12.1(7)E. Support for this command was added for Cisco 7200 VXR routers and Catalyst 6000 family switches.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is supported on the C 10000 router. It is used with the Cisco channelized STM-1 card. Use the tug-2 e1 channel-group timeslots command in configuration controller tug3 command mode to configure a logical channel group on an E1 line that has been mapped to a TUG-3 via the aug mapping au-4 command.

Use the tug-2 e1 channel-group timeslots command in configuration controller au3 command mode to configure a logical channel group on an E1 line that has been mapped to an AU-3 via the aug mapping au-3 command.

Examples

The following example configures logical channel group 15 on E1 1, that is mapped to a TUG-3, and assigns channelized time slots 1 to 5 and 20 to 23 on a Cisco 7500 series router:

```
Router(config)# controller sonet 2/0/0
Router(config-controller)# framing sdh
Router(config-controller)# aug mapping au-4
Router(config-controller)# au-4 1 tug-3 2
Router(config-ctrlr-tug3)# tug-2 4 e1 1 channel group 15 timeslots 1-5, 20-23
```

The following example configures logical channel group 10 on E1 1, that is mapped to an AU-3, and assigns channelized time slots 1 to 5 and 20 to 23 on a Cisco 7200 VXR router or a Catalyst 6000 family switch:

```
Router(config)# controller sonet 2/0
Router(config-controller)# framing sdh
Router(config-controller)# aug mapping au-3
Router(config-controller)# au-3 1
Router(config-ctrlr-au3)# tug-2 4 e1 1 channel group 10 timeslots 1-5, 20-23
```

Related Commands

Command	Description
aug mapping	Configures the AUG mapping mode of the PA-MC-STM-1.
au-3	Configures a particular AU-3 of an E1 line that has been mapped to an AU-3.
au-4 tug-3	Specifies the AU-4 and TUG-3 number of an E1 line that has been mapped to an AU-4.
tug-2 e1 unframed	Creates an unframed (clear channel) logical channel group on an E1 line.
tug-2 e1 framing	Specifies the type of framing used by the E1 lines.

tug-2 e1 clock source

To set the clock source on an E1 line that has been mapped to a TUG-3 or an AU-3, use the **tug-2e1clocksource**command in the appropriate configuration mode.

tug-2 *tug-2-number* **e1** *e1-number* **clock source** {**internal** | **line**}

Syntax Description

tug-2-number	A number in the range of 1 to 7.
e1-number	A number in the range of 1 to 3.
internal	Specifies the PA-MC-STM-1 as the clock source.
line	Specifies the E1 line as the clock source.

Command Default

Clock source is configured from the E1 line.

Command Modes

Configuration controller tug3 (for an E1 line mapped to a TUG-3) Configuration controller au3 (for an E1 line mapped to an AU-3)

Command History

Release	Modification
12.0(14)S	This command was introduced.
12.1(7)E	This command was integrated into Cisco IOS Release 12.1(7)E. Support for this command was added for Cisco 7200 VXR routers and Catalyst 6000 family switches.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the tug-2 e1 clock source command in configuration controller tug3 command mode to configure the clock source of an E1 line that has been mapped to a TUG-3 via the aug mapping au-4 command.

Use the tug-2 e1 clock source command in configuration controller au3 command mode to configure the clock source of an E1 line that has been mapped to an AU-3 via the aug mapping au-3 command.

Examples

The following example configures E1 line 1, that has been mapped to an AU-3 on a Cisco 7200 VXR router or a Catalyst 6000 family switch, to be the clock source:

```
Router(config)# controller sonet 2/0
Router(config-controller)# aug mapping au-3
Router(config-controller)# au-3 1
Router(config-ctrlr-au3)# tug-2 4 e1 1 clock source line
```

The following example configures E1 line 1, that has been mapped to a TUG-3 on a Cisco 7500 series router to use the PA-MC-STM-1, as the clock source:

```
Router(config)# controller sonet 2/0/0
Router(config-controller)# aug mapping au-4
Router(config-controller)# au-4 1 tug-3 2
Router(config-ctrlr-tug3)# tug-2 4 e1 1 clock source internal
```

Related Commands

Command	Description
aug mapping	Configures the AUG mapping mode of the PA-MC-STM-1.
au-3	Configures a particular AU-3 of an E1 line that has been mapped to an AU-3.
au-4 tug-3	Specifies the AU-4 and TUG-3 number of an E1 line that has been mapped to an AU-4.

tug-2 e1 framing

To set the type of framing used by an E1 line that has been mapped to a TUG-3 or an AU-3, use the **tug-2e1framing**command in appropriate configuration mode. To disable the framing mode, user the no form of this command.

tug-2 *tug-2-number* **e1** *e1-number* **framing** {**crc4** | **no-crc4**}
no **tug-2** *tug-2-number* **e1** *e1-number* **framing** {**crc4** | **no-crc4**}

Syntax Description

tug-2-number	A number in the range of 1 to 7.
e1-number	A number in the range of 1 to 3.
crc4	Specifies 4-bit cyclic redundancy check framing.
no-crc4	Specifies basic framing.

Command Default

Framing format is crc4.

Command Modes

Configuration controller tug3 (for an E1 line mapped to a TUG-3) Configuration controller au3 (for an E1 line mapped to an AU-3)

Command History

Release	Modification
12.0(14)S	This command was introduced.
12.1(7)E	This command was integrated into Cisco IOS Release 12.1(7)E. Support for this command was added for Cisco 7200 VXR routers and Catalyst 6000 family switches.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the tug-2 e1 framing command in configuration controller tug3 command mode to configure the type of framing used by an E1 line that has been mapped to a TUG-3 via the aug mapping au-4 command.

Use the tug-2 e1 framing command in configuration controller au3 command mode to configure the type of framing used by an E1 line that has been mapped to an AU-3 via the aug mapping au-3 command.

Examples

The following example configures E1 line 1, that has been mapped to a TUG-3 on a Cisco 7200 VXR router or a Catalyst 6000 family switch, to use crc4 framing:

```
Router(config)# controller sonet 2/0
Router(config-controller)# aug mapping au-4
```

```
Router(config-controller)# au-4 1 tug-3 2
Router(config-ctrlr-tug3)# tug-2 4 e1 1 framing crc4
```

The following example configures E1 line 1, that has been mapped to an AU-3 on a Cisco 7500 series router, to use basic framing:

```
Router(config)# controller sonet 2/0/0
Router(config-controller)# aug mapping au-3
Router(config-controller)# au-3 1
Router(config-ctrlr-au3)# tug-2 4 e1 1 framing no-crc4
```

Related Commands

Command	Description
aug mapping	Configures the AUG mapping mode of the PA-MC-STM-1.
au-3	Configures a particular AU-3 of an E1 line that has been mapped to an AU-3.
au-4 tug-3	Specifies the AU-4 and TUG-3 number of an E1 line that has been mapped to an AU-4.
tug-2 e1 unframed	Creates an unframed (clear channel) logical channel group on an E1 line.

tug-2 e1 loopback

To specify a loopback on an E1 line that has been mapped to a TUG-3 or an AU-3, use the **tug-2e1loopback**command in appropriate configuration mode. To disable the loopback, use the **no** form of this command.

tug-2 *tug-2-number* **e1** *e1-number* **loopback** {**local** | **network** {**line** | **payload**}}
[**no**] **tug-2** *tug-2-number* **e1** *e1-number* **loopback** {**local** | **network** {**line** | **payload**}}

Syntax Description

tug-2-number	A number in the range of 1 to 7.
e1-number	A number in the range of 1 to 3.
local	Loops transmitted E1 output back to the router via the internal E1 framer.
network {**line**| **payload**	Sets the loopback toward the network before going through the framer (**line**) or after going through the framer (payload).

Command Default

No loopbacks are set on an E1 line.

Command Modes

Configuration controller tug3 (for an E1 line mapped to a TUG-3) Configuration controller au3 (for an E1 line mapped to an AU-3

Command History

Release	Modification
12.0(14)S	This command was introduced.
12.1(7)E	This command was integrated into Cisco IOS Release 12.1(7)E. Support for this command was added for Cisco 7200 VXR erouters and Catalyst 6000 family switches.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

TUG-3 Command Mode

Use the tug-2 e1 loopback command in configuration controller tug3 command mode to specify a loopback for an E1 line that has been mapped to a TUG-3 via the aug mapping au-4 command.

AU-3Command Mode

Use the tug-2 e1 loopback command in configuration controller au3 command mode to specify a loopback for an E1 line that has been mapped to an AU-3 via the aug mapping au-3 command.

tug-2 e1 loopback network line|path Command

If you configure a loopback to an e1 interface, it will be be looped as configured. However, if a channel group is configured while the loopback interface is still in configuration, the interface driver will ignore the loopback command in the configuration and the serial interface will be activated.

Examples

E1 Line Mapped to an AU-3 Interface

The following example sets E1 line 1 that has been mapped to an AU-3 on a Cisco 7200 VXR router or a Catalyst 6000 family switch, into network line loopback:

```
Router(config)# controller sonet 2/0
Router(config-controller)# aug mapping au-3
Router(config-controller)# au-3 1
Router(config-ctrlr-au3)# tug-2 4 e1 1 loopback network line
```

E1 Line Mapped to a TUG-3 Interface

The following example sets E1 line 1, that has been mapped to a TUG-3 on a Cisco 7500 series router, into local loopback:

```
Router(config)# controller sonet 2/0/0
Router(config-controller)# aug mapping au-4
Router(config-controller)# au-4 1 tug-3 2
Router(config-ctrlr-tug3)# tug-2 4 e1 1 loopback local
```

Related Commands

Command	Description
aug mapping	Configures the AUG mapping mode of the PA-MC-STM-1.
au-3	Configures a particular AU-3 of an E1 line that has been mapped to an AU-3.
au-4 tug-3	Specifies the AU-4 and TUG-3 number of an E1 line that has been mapped to an AU-4.

tug-2 e1 national bits

To set the national reserved bits on an E1 line that has been mapped to a TUG-3 or an AU-3, use the **tug-2e1nationalbits**command in appropriate configuration mode.

tug-2 *tug-2-number* **e1** *e1-number* **national bits** *pattern*

Syntax Description

tug-2 -umber	A number in the range of 1 to 7.
e1-number	A number in the range of 1 to 3.
pattern	The national reserved bit pattern is a hexadecimal value in the range 0x0 to 0x1F (hexadecimal) or 0 to 31 (decimal).

Command Default

0x1F

Command Modes

Configuration controller tug3 (for an E1 line mapped to a TUG-3) Configuration controller au3 (for an E1 line mapped to an AU-3)

Command History

Release	Modification
12.0(14)S	This command was introduced.
12.1(7)E	This command was integrated into Cisco IOS Release 12.1(7)E. Support for this command was added for Cisco 7200 VXR routers and Catalyst 6000 family switches.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the tug-2 e1 national bits command in configuration controller tug3 command mode to configure the national reserved bits for an E1 line that has been mapped to a TUG-3 via the aug mapping au-4 command.

Use the tug-2 e1 national bits command in configuration controller au3 command mode to configure the national reserved bits for an E1 line that has been mapped to an AU-3 via the aug mapping au-3 command.

Examples

The following example configures the national reserved bits for E1 line 1, that has been mapped to a TUG-3 on a Cisco 7200 VXR router or a Catalyst 6000 family switch, into a 0x0 hexadecimal pattern:

```
Router(config)# controller sonet 2/0
Router(config-controller)# aug mapping au-4
Router(config-controller)# au-4 1 tug-3 2
Router(config-ctrlr-tug3)# tug-2 4 e1 1 national bits 0x0
```

The following example configures the national reserved bits for E1 line 1, that has been mapped to an AU-3 on a Cisco 7500 series router, into decimal pattern 0:

```
Router(config)# controller sonet 2/0/0
Router(config-controller)# aug mapping au-3
Router(config-controller)# au-3 1
Router(config-ctrlr-au3)# tug-2 4 e1 1 national bits 0
```

Related Commands

Command	Description
aug mapping	Configures the AUG mapping mode of the PA-MC-STM-1.
au-3	Configures a particular AU-3 of an E1 line that has been mapped to an AU-3.
au-4 tug-3	Specifies the AU-4 and TUG-3 number of an E1 line that has been mapped to an AU-4.

tug-2 e1 shutdown

To shut down an individual E1 line that has been mapped to a TUG-3 or an AU-3, use the **tug-2e1shutdown**command in appropriate configuration mode. To enable an individual E1 line, use the **no** form of this command.

tug-2 *tug-2-number* **e1** *e1-number* **shutdown**
[**no**] **tug-2** *tug-2* *number* **e1** *e1-number* **shutdown**

Syntax Description

tug-2-number	A number in the range of 1 to 7.
e1-number	A number in the range of 1 to 3.

Command Default

E1 lines are not shut down.

Command Modes

Configuration controller tug3 (for an E1 line mapped to a TUG-3) Configuration controller au3 (for an E1 line mapped to an AU-3

Command History

Release	Modification
12.0(14)S	This command was introduced.
12.1(7)E	This command was integrated into Cisco IOS Release 12.1(7)E. Support for this command was added for Cisco 7200 VXR routers and Catalyst 6000 family switches.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the tug-2 e1 shutdown command in configuration controller tug3 command mode to shut down an individual E1 line that has been mapped to a TUG-3 via the aug mapping au-4 command.

Use the tug-2 e1 shutdown command in configuration controller au3 command mode to shut down an individual E1 line that has been mapped to an AU-3 via the aug mapping au-3 command.

Examples

The following example shuts down E1 line 1 that has been mapped to an AU-3 on a Cisco 7200 VXR router or a Catalyst 6000 family switch:

```
Router(config)# controller sonet 2/0
Router(config-controller)# aug mapping au-3
Router(config-controller)# au-3 1
Router(config-ctrlr-au3)# tug-2 4 e1 1 shutdown
```

The following example shuts down E1 line 1, that has been mapped to a TUG-3 on a Cisco 7500 series router:

```
Router(config)# controller sonet 2/0/0
Router(config-controller)# aug mapping au-4
Router(config-controller)# au-4 1 tug-3 2
Router(config-ctrlr-tug3)# tug-2 4 e1 1 shutdown
```

Related Commands

Command	Description
aug mapping	Configures the AUG mapping mode of the PA-MC-STM-1.
au-3	Configures a particular AU-3 of an E1 line that has been mapped to an AU-3.
au-4 tug-3	Specifies the AU-4 and TUG-3 number of an E1 line that has been mapped to an AU-4.

tug-2 e1 unframed

To create an E1 unframed (clear channel) logical channel group on an E1 line that has been mapped to a TUG-3 or an AU-3, use the **tug-2e1unframed**command in appropriate configuration mode. To remove a logical channel group, use the **no** form of this command.

tug-2 *tug-2-number* **e1** *e1-number* **unframed**
[**no**] **tug-2** *tug-2-number* **e1** *e1-number* **unframed**

Syntax Description

tug-2 -umber	A number in the range of 1 to 7.
e1-number	A number in the range of 1 to 3.

Command Default

No default behavior or values.

Command Modes

Configuration controller tug3 (for an E1 line mapped to a TUG-3) Configuration controller au3 (for an E1 line mapped to an AU-3)

Command History

Release	Modification
12.0(14)S	This command was introduced.
12.1(7)E	This command was integrated into Cisco IOS Release 12.1(7)E. Support for this command was added for Cisco 7200 VXR routers and Catalyst 6000 family switches.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the tug-2 e1 unframed command in configuration controller tug3 command mode to create an unframed (clear channel) logical channel group on an E1 line that has been mapped to a TUG-3 via the aug mapping au-4 command.

Use the tug-2 e1 unframed command in configuration controller au3 command mode to create an unframed (clear channel) logical channel group on an E1 line that has been mapped to an AU-3 via the aug mapping au-3 command.

The channel group number for unframed E1 lines is always 0.

Examples

The following example configures an unframed logical channel group on E1 line 1 that has been mapped to a TUG-3 on a Cisco 7200 VXR router or a Catalyst 6000 family switch:

```
Router(config)# controller sonet 2/0
Router(config-controller)# aug mapping au-4
```

```
Router(config-controller)# au-4 1 tug-3 2
Router(config-ctrlr-tug3)# tug-2 4 e1 1 unframed
```

The following example configures an unframed logical channel group on E1 line 1 that has been mapped to an AU-3 on a Cisco 7500 series router:

```
Router(config)# controller sonet 2/0/0
Router(config-controller)# aug mapping au-3
Router(config-controller)# au-3 1
Router(config-ctrlr-au3)# tug-2 4 e1 1 unframed
```

Related Commands

Command	Description
aug mapping	Configures the AUG mapping mode of the PA-MC-STM-1.
au-3	Configures a particular AU-3 of an E1 line that has been mapped to an AU-3.
au-4 tug-3	Specifies the AU-4 and TUG-3 number of an E1 line that has been mapped to an AU-4.

tug-3

Use this command to configure mode Tributary Unit group type 3 (TUG-3) number that has been mapped to an AU-4.

tug-3 *tug-3 number*

Syntax Description

Syntax Description

tug-3 number	The range is from 1 to 3.

Command Default

None

Command Modes

Controller configuration

Command History

Release	Modification
XE Everest 16.6.1	This command was integrated into the Cisco NCS 4200 Series and Cisco ASR 900 Series.

Usage Guidelines

An AUG of an STM-1 can be derived from either AU-3s or an AU-4. Use the **aug mapping au-4** configuration controller command to map the AUG to a TUG-3. Configuring the **au-4** command enables you to enter configuration controller tug3 command mode and creates a serial interface.

Examples

```
enable
configure terminal
controller sdh 0/5/0
rate stm4
au-4 1
mode tug-3
tug-3 1
mode t3
cem-group 100 unframed
end
```

Related Commands

Command	Description
show running configuration	Verifies TUG-3 configuration.

tunnel bandwidth through yellow

tunnel bandwidth

To set the transmit bandwidth used by the tunnel interface, use the **tunnelbandwidth** command in interface configuration mode. To restore the default setting, use the no form of this command.

tunnel bandwidth {**receive** | **transmit**} *bandwidth*
no tunnel bandwidth

Syntax Description

receive	Specifies the bandwidth to be used to receive packets through the tunnel. **Note** This keyword is no longer used and will be removed in future releases.
transmit	Specifies the bandwidth to be used to send packets through the tunnel.
bandwidth	Bandwidth, in kbps. Range is from 0 to 2147483647. Default is 8000.

Command Default

8000 kbps

Command Modes

Interface configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

Use the **tunnelbandwidth** command to specify the capacity of the satellite link.

Examples

The following example shows how to set the satellite tunnel bandwidth to 1000 kbps for transmitting packets using Rate Based Satellite Control Protocol:

```
Router(config
)
# interface tunnel 0
Router(config
-if)#
 tunnel bandwidth transmit 1000
```

Related Commands

Command	Description
tunnel destination	Specifies the destination for a tunnel interface.
tunnel mode	Sets the encapsulation mode for a tunnel interface.
tunnel source	Sets the source address of a tunnel interface.

tunnel checksum

To enable encapsulator-to-decapsulator checksumming of packets on a tunnel interface, use the **tunnelchecksum**command in interface configuration mode. To disable checksumming, use the **no** form of this command.

tunnel checksum
no tunnel checksum

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command currently applies to generic routing encapsulation (GRE) only. Some passenger protocols rely on media checksums to provide data integrity. By default, the tunnel does not guarantee packet integrity. By enabling end-to-end checksums, the routers will drop corrupted packets.

Examples

The following example shows how to enable encapsulator-to-decapsulator checksumming of packets for all protocols on the tunnel interface:

```
Router(config
-if)
# tunnel checksum
```

tunnel mpls-ip-only

To copy the inner IP header's Do Not Fragment bit from the payload into the tunnel packet's IP header, use the **tunnel mpls-ip-only** command in the interface configuration mode.

tunnel mpls-ip-only
no tunnel mpls-ip-only

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
17.5.1	This command was introduced.

Usage Guidelines

If the Do Not Fragment bit is not set, the payload is fragmented when the IP packet exceeds the MTU set for the interface. When you enable the **tunnel mpls-ip-only** command, the **tunnel path-mtu-discovery** automatically gets enabled due to the dependency.

Examples

The following example shows how to enable this command:

```
Router(config-if)# tunnel mpls-ip-only
```

tunnel destination

To specify the destination for a tunnel interface, use the **tunnel destination** command in interface configuration mode. To remove the destination, use the **no** form of this command.

tunnel destination {*host-nameip-addressipv6-address* | **dynamic**}
no tunnel destination

Command Syntax for Cisco Catalyst 3850 Series Switches

tunnel destination *ip-address*
no tunnel destination

Syntax Description

host-name	Name of the host destination.
ip-address	IP address of the host destination expressed in dotted decimal notation.
ipv6-address	IPv6 address of the host destination expressed in IPv6 address format.
dynamic	Applies the tunnel destination address dynamically to the tunnel interface.

Command Default

No tunnel interface destination is specified.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
12.3(7)T	This command was modified. The address field was modified to accept an *ipv6-address* argument to allow IPv6 nodes to be configured as a tunnel destination.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1SY	This command was integrated into Cisco IOS Release 15.1SY.
Cisco IOS XE Release 3.7S	This command was modified. The **dynamic** keyword was added.

Release	Modification
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

You cannot configure two tunnels to use the same encapsulation mode with exactly the same source and destination addresses. The workaround is to create a loopback interface and configure the packet source off of the loopback interface. Refer to the *Cisco IOS AppleTalk*, *ISO CLNS*, *and Novell IPX Configuration Guide* for more information about AppleTalk Cayman tunneling.

Note **Only GRE tunneling is supported on Cisco Catalyst 3850 Series Switches.**

Tunnel Destination Address for Cayman Tunnel

The following example shows how to configure the tunnel destination address for Cayman tunneling:

```
Device(config)# interface tunnel0
Device(config-if)# tunnel source ethernet0
Device(config-if)# tunnel destination 10.108.164.19
Device(config-if)# tunnel mode cayman
```

Tunnel Destination Address for Dynamic Tunnel

The following example shows how to set the tunnel destination address dynamically:

```
Device(config)# interface tunnel0
Device(config-if)# tunnel destination dynamic
Device(config-if)# *Nov 22 19:38:28.271: Tunnel notified destination change: dynamic is set
Device(config-if)# end
Device# show run interface tunnel0
Building configuration...

Current configuration : 63 bytes
!
interface Tunnel0
 no ip address
 tunnel source dynamic
 tunnel destination dynamic
end
```

If the tunnel destination address is configured to be set dynamically, you cannot configure the tunnel destination address without removing the dynamic configuration.

```
Device(config)# interface tunnel0
Device(config-if)# tunnel destination ethernet 0/0
Device(config-if)# end
Device# show run interface tunnel0
Building configuration...

Current configuration : 63 bytes
!
interface Tunnel0
```

```
 no ip address
 tunnel destination dynamic
end
Device# configure terminal
Device(config)# interface tunnel0
Device(config-if)# no tunnel destination
```

Tunnel Destination Address for GRE Tunneling

The following example shows how to configure the tunnel destination address for generic routing encapsulation (GRE) tunneling:

```
Device(config)# interface tunnel0
Device(config-if)# appletalk cable-range 4160-4160 4160.19
Device(config-if)# appletalk zone Engineering
Device(config-if)# tunnel source ethernet0
Device(config-if)# tunnel destination 10.108.164.19
Device(config-if)# tunnel mode gre ip
```

Tunnel Destination Address for GRE Tunneling on Cisco Catalyst 3850 Series Switches

The following example shows how to configure the logical Layer 3 GRE tunnel interface tunnel 2 in Global or non- VRF environment on Cisco Catalyst 3850 Series Switches:

```
Device(config)# interface tunnel 2
Device(config-if)# ip address 100.1.1.1 255.255.255.0
Device(config-if)# tunnel source 10.10.10.1
Device(config-if)# tunnel destination 10.10.10.2
Device(config-if)# tunnel mode gre ip
Device(config-if)# end
```

The following example shows how to configure the logical Layer 3 GRE tunnel interface tunnel 2 in VRF environment on Cisco Catalyst 3850 Series Switches. Use the **vrf definition** *vrf-name* and the**vrf forwarding** *vrf-name* commands to configure and apply VRF.

```
Device(config)# vrf definition RED
Device(config-vrf)#  address-family ipv4
Device(config-vrf-af)# exit-address-family
Device(config-vrf)#  exit
Device(config)# interface tunnel 2
Device(config)# vrf forwarding RED
Device(config-if)# ip address 100.1.1.1 255.255.255.0
Device(config-if)# tunnel source 10.10.10.1
Device(config-if)# tunnel destination 10.10.10.2
Device(config-if)# tunnel mode gre ip
Device(config-if)# end
```

Tunnel Destination Address for IPv6 Tunnel

The following example shows how to configure the tunnel destination address for GRE tunneling of IPv6 packets:

```
Device(config)# interface Tunnel0
Device(config-if)# no ip address
Device(config-if)# ipv6 router isis
```

```
Device(config-if)# tunnel source Ethernet0/0
Device(config-if)# tunnel destination 2001:0DB8:1111:2222::1/64
Device(config-if)# tunnel mode gre ipv6
Device(config-if)# exit
!
Device(config)# interface Ethernet0/0
Device(config-if)# ip address 10.0.0.1 255.255.255.0
Device(config-if)# exit
!
Device(config)# ipv6 unicast-routing
Device(config)# router isis
Device(config)# net 49.0000.0000.000a.00
```

Note **IPv6 GRE tunneling is not supported on Cisco Catalyst 3850 Series Switches.**

Related Commands

Command	Description
appletalk cable-range	Enables an extended AppleTalk network.
appletalk zone	Sets the zone name for the connected AppleTalk network.
tunnel mode	Sets the encapsulation mode for the tunnel interface.
tunnel source	Sets the source address of a tunnel interface.

tunnel endpoint service-policy output

To configure a Quality of Service (QoS) policy for a tunnel in an output direction, use the **tunnel endpoint service-policy output** command in configuration interface mode. To remove the QoS policy for a tunnel, use the **no** form of the command.

tunnel endpoint service-policy output *policy-name*

Syntax Description

policy-name	Name of the policy map to associate with a tunnel.

Command Default

By default no policy is configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE 13.3S	This command was introduced.

Usage Guidelines

Use the **tunnel endpoint service policy output** command to associate a service policy with Ethernet over GRE (EoGRE) tunnels. Use the **policy-map** command in global configuration mode, to create a policy map.

The following example shows how to configure a Quality of Service (QoS) policy for outward traffic on a tunnel:

```
Device(config)# interface tunnel 1
Device(config-if)# tunnel source Loopback 0
Device(config-if)# tunnel vlan 10, 20
Device(config-if)# ip address unnumbered Loopback 0
Device(config-if)# tunnel mode ethernet gre ipv4
Device(config-if)# tunnel endpoint service-policy output tunnel-qos-policy
Device(config-if)# ip subscriber l2-connected
Device(config-subscriber)# initiator unclassified mac-address
Device(config-subscriber)# initiator dhcp
Device(config-subscriber)# exit
```

Related Commands

Command	Description
policy-map	Creates a policy map that can be attached to one or more interfaces.
show policy-map multipoint tunnel	Displays information about a specific QoS policy for a multipoint tunnel interface.

tunnel entropy

To achieve load balancing of tunnel packets in a network, use the **tunnel entropy** command in interface configuration mode. To stop load balancing, use the **no** form of the command.

tunnel entropy

no tunnel entropy

Command Default

Calculation of tunnel entropy is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.11S	This command was introduced.

Usage Guidelines

You can enable tunnel entropy calculation only in Generic Routing Encapsulation (GRE) mode. If you configure a 32-bit tunnel key, you must remove the existing key first.

To disable tunnel entropy calculation, you must remove the configured tunnel key before using the **no tunnel entropy** command to disable entropy calculation.

Use the **show interfaces tunnel** command to verify whether tunnel entropy calculation is enabled or not. If it is enabled, the key size is also displayed.

Example

The following example shows how to configure tunnel entropy calculation for GRE mode of the tunnel interface:

```
Device> enable
Device# configure terminal
Device(config)# interface tunnel 21
Device(config-if)# tunnel source 10.1.1.1
Device(config-if)# tunnel destination 172.168.2.1
Device(config-if)# tunnel mode gre ip
Device(config-if)# tunnel key 4683
Device(config-if)# tunnel entropy
Device(config-if)# end
```

The following is sample output from the **show interfaces tunnel** command, which displays that tunnel entropy calculation is enabled with a 24-bit key:

```
Device# show interfaces tunnel 21

Tunnel21 is up, line protocol is up
Hardware is Tunnel
MTU 17864 bytes, BW 100 Kbit/sec, DLY 50000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel source 10.1.1.1, destination 172.168.2.1
```

```
Tunnel protocol/transport GRE/IP
Key 0x124B, sequencing disabled
Checksumming of packets disabled
Tunnel Entropy Calculation Enabled (24-bit Key)
Tunnel TTL 255, Fast tunneling enabled
Tunnel transport MTU 1472 bytes
Tunnel transmit bandwidth 8000 (kbps)
Tunnel receive bandwidth 8000 (kbps)
Last input never, output never, output hang never
Last clearing of "show interface" counters 00:03:07
Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/0 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 unknown protocol drops
0 output buffer failures, 0 output buffers swapped out
```

Related Commands

Command	Description
show interfaces	Displays statistics for all interfaces configured on a device or access server.
show ip route	Displays the current state of the routing table.

tunnel key

To enable an ID key for a tunnel interface, use the**tunnelkey** command in interface configuration mode. To remove the ID key, use the **no** form of this command.

tunnel key *key-number*
no tunnel key

Syntax Description

key-number	Number from 0 to 4294967295 that identifies the tunnel key.

Command Default

No tunnel ID keys are enabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.11S	This command was integrated into Cisco IOS XE Release 3.11S.

Usage Guidelines

This command currently applies to generic route encapsulation (GRE) only. Tunnel ID keys can be used as a form of *weak* security to prevent improper configuration or injection of packets from a foreign source.

Note IP multicast traffic is not supported when a tunnel ID key is configured unless the traffic is process-switched. You must configure the **noipmroute-cache** command in interface configuration mode on the interface if an ID key is configured. This note applies only to Cisco IOS Release 12.0 and earlier releases.

Note When GRE is used, the ID key is carried in each packet. We do *not* recommend relying on this key for security purposes.

Examples

The following example shows how to set the tunnel ID key to 3:

```
Device(config-if)# tunnel key 3
```

tunnel mode

To set the encapsulation mode for the tunnel interface, use the **tunnel mode** command in interface configuration mode. To return to the default mode, use the **no** form of this command.

tunnel mode {**aurp** | **cayman** | **dvmrp** | **eon** | **ethernet gre** {**ipv4** | **ipv6**} | **gre** | **gre multipoint** | **gre ipv6** | **ipip** [**decapsulate-any**] | **ipsec ipv4** | **iptalk** | **ipv6** | **ipsec ipv6** | **mpls** | **nos** | **rbscp** }
no tunnel mode

Command Syntax for Cisco Catalyst 3850 Series Switches

tunnel mode gre ip
no tunnel mode

Syntax Description

aurp	AppleTalk Update-Based Routing Protocol.
cayman	Cayman TunnelTalk AppleTalk encapsulation.
dvmrp	Distance Vector Multicast Routing Protocol (DMVRP).
ethernet gre ipv4	Ethernet over Generic Routing Encapsulation (GRE) IPv4.
ethernet gre ipv6	Ethernet over GRE IPv6.
eon	EON–compatible Connectionless Network Service (CLNS) tunnel.
gre	GRE protocol. This is the default.
gre multipoint	Multipoint GRE (mGRE).
gre ipv6	GRE tunneling using IPv6 as the delivery protocol.
ipip	IP-over-IP encapsulation.
decapsulate-any	(Optional) Terminates any number of IP-in-IP tunnels at one tunnel interface. This tunnel will not carry any outbound traffic; however, any number of remote tunnel endpoints can use a tunnel configured this way as their destination.
ipsec ipv4	Tunnel mode is IPSec, and the transport is IPv4.
iptalk	Apple IPTalk encapsulation.
ipv6	Static tunnel interface configured to encapsulate IPv6 or IPv4 packets in IPv6.
ipsec ipv6	Tunnel mode is IPSec, and the transport is IPv6.
mpls	Multiprotocol Label Switching (MPLS) encapsulation.
nos	KA9Q/NOS–compatible IP over IP.
rbscp	Rate Based Satellite Control Protocol (RBSCP).

Command Default

The default is GRE tunneling.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
10.3	This command was modified. The **aurp**, **dvmrp**, and **ipip** keywords were added.
11.2	This command was modified. The optional **decapsulate-any** keyword was added.
12.2(13)T	This command was modified. The **gre multipoint** keyword was added.
12.3(7)T	This command was modified. The following keywords were added: • **gre ipv6** to support GRE tunneling using IPv6 as the delivery protocol. • **ipv6** to allow a static tunnel interface to be configured to encapsulate IPv6 or IPv4 packets in IPv6. • **rbscp** to support RBSCP.
12.3(14)T	This command was modified. The **ipsec ipv4** keyword was added.
12.2(18)SXE	This command was modified. The **gre multipoint** keyword was added.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.4(4)T	This command was modified. The **ipsec ipv6** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 Series Routers.
15.1SY	This command was integrated into Cisco IOS Release 15.1SY.
Cisco IOS XE Release 3.9S	This command was modified. The **ethernet gre** keyword was added.

Usage Guidelines

Source and Destination Address

You cannot have two tunnels that use the same encapsulation mode with exactly the same source and destination address. The workaround is to create a loopback interface and source packets off of the loopback interface.

Cayman Tunneling

Designed by Cayman Systems, Cayman tunneling enables tunneling to enable Cisco routers to interoperate with Cayman GatorBoxes. With Cayman tunneling, you can establish tunnels between two routers or between a Cisco router and a GatorBox. When using Cayman tunneling, you must not configure the tunnel with an AppleTalk network address.

DVMRP

Use DVMRP when a router connects to an mrouted (multicast) router to run DVMRP over a tunnel. You must configure Protocol Independent Multicast (PIM) and an IP address on a DVMRP tunnel.

Ethernet over GRE

Use Ethernet over GRE to send ethernet traffic from low-end resident gateways (RGs) or Customer Premises Equipment (CPE) to aggregation routers where Mobile Access Gateway (MAG) is enabled over GRE tunnels. The RGs and CPE can then provide mobility services to mobile nodes (MNs).

GRE with AppleTalk

GRE tunneling can be done between Cisco routers only. When using GRE tunneling for AppleTalk, you configure the tunnel with an AppleTalk network address. Using the AppleTalk network address, you can ping the other end of the tunnel to check the connection.

Multipoint GRE

After enabling mGRE tunneling, you can enable the **tunnel protection** command, which allows you to associate the mGRE tunnel with an IPSec profile. Combining mGRE tunnels and IPSec encryption allows a single mGRE interface to support multiple IPSec tunnels, thereby simplifying the size and complexity of the configuration.

Note GRE tunnel keepalives configured using the **keepalive** command under a GRE interface are supported only on point-to-point GRE tunnels.

RBSCP

RBSCP tunneling is designed for wireless or long-distance delay links with high error rates, such as satellite links. Using tunnels, RBSCP can improve the performance of certain IP protocols, such as TCP and IPSec, over satellite links without breaking the end-to-end model.

IPsec in IPv6 Transport

IPv6 IPsec encapsulation provides site-to-site IPsec protection of IPv6 unicast and multicast traffic. This feature allows IPv6 routers to work as a security gateway, establishes IPsec tunnels to another security gateway router, and provides crypto IPsec protection for traffic from an internal network when it is transmitted across the public IPv6 Internet. IPv6 IPsec is very similar to the security gateway model using IPv4 IPsec protection.

Note **Only GRE tunneling is supported on Cisco Catalyst 3850 Series Switches.**

Cayman Tunneling

The following example shows how to enable Cayman tunneling:

```
Device(config)# interface tunnel 0
Device(config-if)# tunnel source ethernet 0
Device(config-if)# tunnel destination 10.108.164.19
Device(config-if)# tunnel mode cayman
```

Ethernet over GRE Tunneling

The following example shows how to enable Ethernet over GRE tunneling for IPv6:

```
Device(config)# interface tunnel 0
Device(config)# mac-address 0000.0000.00001
Device(config-if)# ip address 10.1.1.2 255.255.255.0
Device(config-if)# tunnel source Loopback0
Device(config-if)# tunnel mode gre ipv6
Device(config-if)# tunnel vlan 1023
```

GRE Tunneling

The following example shows how to enable GRE tunneling:

```
Device(config)# interface tunnel 0
Device(config-if)# appletalk cable-range 4160-4160 4160.19
Device(config-if)# appletalk zone Engineering
Device(config-if)# tunnel source ethernet0
Device(config-if)# tunnel destination 10.108.164.19
Device(config-if)# tunnel mode gre
```

GRE Tunneling Examples for Cisco Catalyst 3850 Series Switches

The following example shows how to configure the logical Layer 3 GRE tunnel interface tunnel 2 in Global or non- VRF environment on Cisco Catalyst 3850 Series Switches:

```
Device(config)# interface tunnel 2
Device(config-if)# ip address 100.1.1.1 255.255.255.0
Device(config-if)# tunnel source 10.10.10.1
Device(config-if)# tunnel destination 10.10.10.2
Device(config-if)# tunnel mode gre ip
Device(config-if)# end
```

The following example shows how to configure the logical Layer 3 GRE tunnel interface tunnel 2 in VRF environment on Cisco Catalyst 3850 Series Switches. Use the **vrf definition** *vrf-name* and the**vrf forwarding** *vrf-name* commands to configure and apply VRF.

```
Device(config)# vrf definition RED
Device(config-vrf)#  address-family ipv4
Device(config-vrf-af)# exit-address-family
Device(config-vrf)#  exit
Device(config)# interface tunnel 2
Device(config)# vrf forwarding RED
Device(config-if)# ip address 100.1.1.1 255.255.255.0
Device(config-if)# tunnel source 10.10.10.1
Device(config-if)# tunnel destination 10.10.10.2
Device(config-if)# tunnel mode gre ip
Device(config-if)# end
```

Note **IPv6 GRE tunneling is not supported on Cisco Catalyst 3850 Series Switches.**

IPsec in IPv4 Transport

The following example shows how to configure a tunnel using IPsec encapsulation with IPv4 as the transport mechanism:

```
Device (config)# crypto ipsec profile PROF
Device (config)# set transform tset
Device (config)# interface tunnel 0
Device (config-if)# ip address 10.1.1.1 255.255.255.0
Device (config-if)# tunnel mode ipsec ipv4
Device (config-if)# tunnel source loopback 0
Device (config-if)# tunnel destination 172.16.1.1
```

IPsec in IPv6 Transport

The following example shows how to configure an IPv6 IPsec tunnel interface:

```
Device(config)# interface tunnel 0
Device(config-if)# ipv6 address 2001:0DB8:1111:2222::2/64
Device(config-if)# tunnel destination 10.0.0.1
Device(config-if)# tunnel source Ethernet 0/0
Device(config-if)# tunnel mode ipsec ipv6
Device(config-if)# tunnel protection ipsec profile profile1
```

Multipoint GRE Tunneling

The following example shows how to enable mGRE tunneling:

```
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.1 255.255.255.0
! Ensures longer packets are fragmented before they are encrypted; otherwise, the ! receiving
 router would have to do the reassembly.
 ip mtu 1416
! Turns off split horizon on the mGRE tunnel interface; otherwise, EIGRP will not ! advertise
 routes that are learned via the mGRE interface back out that interface.
 no ip split-horizon eigrp 1
 no ip next-hop-self eigrp 1
 delay 1000
! Sets IPSec peer address to Ethernet interface’s public address.
 tunnel source Ethernet0
 tunnel mode gre multipoint
! The following line must match on all nodes that want to use this mGRE tunnel.
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
```

RBSCP Tunneling

The following example shows how to enable RBSCP tunneling:

```
Device(config)# interface tunnel 0
```

```
Device(config-if)# tunnel source ethernet 0
Device(config-if)# tunnel destination 10.108.164.19
Device(config-if)# tunnel mode rbscp
```

Related Commands

Command	Description
appletalk cable-range	Enables an extended AppleTalk network.
appletalk zone	Sets the zone name for the connected AppleTalk network.
mac-address	Specifies a MAC address to use as the common router MAC address for interfaces on the active and standby chassis.
tunnel destination	Specifies the destination for a tunnel interface.
tunnel protection	Associates a tunnel interface with an IPsec profile.
tunnel source	Sets the source address of a tunnel interface.
tunnel vlan	Associates a VLAN ID for the Ethernet over GRE tunnel interface.

tunnel path-mtu-discovery

To enable Path MTU Discovery (PMTUD) on a generic routing encapsulation (GRE) or IP-in-IP tunnel interface, use the **tunnelpath-mtu-discovery** command in interface configuration mode. To disable PMTUD on a tunnel interface, use the no form of this command.

tunnel path-mtu-discovery [{**age-timer** {*aging-mins* | **infinite**} | **min-mtu** *mtu-bytes*}]
no tunnel path-mtu-discovery

Syntax Description

age-timer	(Optional) Sets a timer to run for a specified interval, in minutes, after which the tunnel interface resets the maximum transmission unit (MTU) of the path to the default tunnel MTU minus 24 bytes for GRE tunnels or minus 20 bytes for IP-in-IP tunnels. • *aging-mins* --Number of minutes. Range is from 10 to 30. Default is 10. • **infinite** -- Disables the age timer.
min-mtu	(Optional) Specifies the minimum Path MTU across GRE tunnels. • *mtu-bytes*-- Number of bytes. Range is from 92 to 65535. Default is 92.

Command Default

Path MTU Discovery is disabled for a tunnel interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)WC5	This command was introduced.
12.0(7)T3	This command was integrated into Cisco IOS Release 12.0(7)T3.
12.2(13)T	The **min-mtu** keyword and *mtu-bytes* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When PMTUD (RFC 1191) is enabled on a tunnel interface, the router performs PMTUD processing for the GRE (or IP-in-IP) tunnel IP packets. The router always performs PMTUD processing on the original data IP packets that enter the tunnel. When PMTUD is enabled, no packet fragmentation occurs on the encapsulated packets that travel through the tunnel. Without packet fragmentation, there is a better throughput of TCP connections, and this makes PMTUD a method for maximizing the use of available bandwidth in the network between the endpoints of a tunnel interface.

After PMTUD is enabled, the Don’t Fragment (DF) bit of the IP packet header that is forwarded into the tunnel is copied to the IP header of the external IP packets. The external IP packet is the encapsulating IP packet. Adding the DF bit allows the PMTUD mechanism to work on the tunnel path of the tunnel. The tunnel endpoint listens for Internet Control Message Protocol (ICMP) unreachable too-big messages and modifies the IP MTU of the tunnel interface, if required.

When the aging timer is configured, the tunnel code resets the tunnel MTU after the aging timer expires. After the tunnel MTU is reset, a set of full-size packets with the DF bit set is required to trigger the tunnel PMTUD and lower the tunnel MTU. At least two packets are dropped each time the tunnel MTU changes.

When PMTUD is disabled, the DF bit of an external (encapsulated) IP packet is set to zero even if the encapsulated packet has a DF bit set to one.

The *min-mtu* argument sets a low limit on the MTU that can be learned via the PMTUD process. Any ICMP signaling received specifying an MTU less than the minimum MTU configured will be ignored. This feature can be used to prevent a denial of service attack from any node that can send a specially crafted ICMP message to the router, specifying a very small MTU. For more information, see "*Crafted ICMP Messages Can Cause Denial of Service* " at the following URL:

http://www.cisco.com/en/US/products/products_security_advisory09186a0080436587.shtml

Note PMTUD on a tunnel interface requires that the tunnel endpoint be able to receive ICMP messages generated by routers in the path of the tunnel. Check that ICMP messages can be received before using PMTUD over firewall connections.

PMTUD works only on GRE and IP-in-IP tunnel interfaces.

Use the **showinterfacestunnel** command to verify the tunnel PMTUD parameters.

Examples

The following example shows how to enable tunnel PMTUD:

```
Router(config)# interface tunnel 0
Router(config-if)# tunnel path-mtu-discovery
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
show interfaces tunnel	Displays information about the specified tunnel interface.

tunnel rbscp ack_split

To enable TCP acknowledgement (ACK) splitting for Rate Based Satellite Control Protocol (RBSCP) tunnels, use the **tunnelrbscpack_split** command in interface configuration mode. To disable TCP acknowledgement splitting for RBSCP tunnels, use the **no** form of this command.

tunnel rbscp ack_split *split-size*
no tunnel rbscp ack_split *split-size*

Syntax Description

split-size	Number of ACKs to send for every ACK received. Range is from 1 to 32. Default is 4.

Command Default

TCP acknowledgement splitting for RBSCP tunnels is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

Performance improvements can be made for clear-text TCP traffic using ACK splitting where a number of additional TCP ACKs are generated for each TCP ACK received. TCP will open a congestion window by one maximum transmission unit (MTU) for each TCP ACK received. Opening the congestion window results in increased bandwidth becoming available. Use the **tunnelrbscpack_split** command only when the satellite link is not using all the available bandwidth. Encrypted traffic cannot use ACK splitting.

Examples

The following example shows how to enable RBSCP tunnel TCP ACK splitting and configure three ACK packets to be sent for each ACK packet received:

```
Router(config
)
# interface tunnel 0
Router(config
-if)#
 tunnel rbscp ack_split 3
```

Related Commands

Command	Description
show rbscp	Displays state and statistical information about RBSCP tunnels.

tunnel rbscp delay

To enable the Rate Based Satellite Control Protocol (RBSCP) tunnel delay, use the **tunnelrbscpdelay** command in interface configuration mode. To disable RBSCP tunnel delay, use the **no** form of this command.

tunnel rbscp delay
no tunnel rbscp delay

Syntax Description

This command has no arguments or keywords.

Command Default

RBSCP tunnel delay is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

Use the **tunnelrbscpdelay** command only if the RBSCP tunnel has a round-trip time (RTT) over 700 milliseconds.

Examples

The following example shows how to enable the RBSCP tunnel delay:

```
Router(config
)
# interface tunnel 0
Router(config
-if)#
 tunnel rbscp delay
```

Related Commands

Command	Description
show rbscp	Displays state and statistical information about RBSCP tunnels.

tunnel rbscp input_drop

To configure the input queue size on a Rate Based Satellite Control Protocol (RBSCP) tunnel, use the **tunnelrbscpinput_drop** command in interface configuration mode. To restore the default input queue size, use the **no** form of this command.

tunnel rbscp input_drop *bw-delay-products*
no tunnel rbscp input_drop

Syntax Description

bw-delay-products	Number of bandwidth delay products (BDP) bytes that can be queued before packets are dropped on the input side. Range from 1 to 10. Default is 2.

Command Default

Input queue size is 2 BDP bytes.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

Use the **tunnelrbscpinput_drop** command to restrict the amount of data queued by the router. After the configured byte limit is reached, packets that would be encapsulated and sent via the tunnel are dropped on the input side. Congestion control of the satellite link is also provided by this command because the dropped packets will force the end hosts to reduce their sending rate of packets.

Use this command in conjunction with the **tunnelrbscplong_drop** command which allows packets that are waiting in an RBSCP tunnel encapsulation queue to be dropped after a period of time.

Examples

The following example shows how to set the RBSCP tunnel queue size to 5 BDP bytes:

```
Router(config
)
# interface tunnel 0
Router(config
-if)#
 tunnel rbscp input_drop 5
```

Related Commands

Command	Description
show rbscp	Displays state and statistical information about RBSCP tunnels.
tunnel rbscp long_drop	Allows packets to be dropped after waiting in the RBSCP tunnel encapsulation queue for too long.

tunnel rbscp long_drop

To allow packets to be dropped that have been queued too long for Rate Based Satellite Control Protocol (RBSCP) tunnel encapsulation, use the **tunnelrbscplong_drop** command in interface configuration mode. To disable the dropping of queued packets, use the **no** form of this command.

tunnel rbscp long_drop
no tunnel rbscp long_drop

Syntax Description

This command has no arguments or keywords.

Command Default

No queued packets are dropped.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

The **tunnelrbscplong_drop** command allows the transmitting router to drop packets that have been waiting in the queue for RBSCP tunnel encapsulation for a long time. The period of time after which packets are dropped is determined using the round-trip time (RTT) estimate of the tunnel.

Use this command in conjunction with the **tunnelrbscpinput_drop** command which configures the size of the input queue. After the configured byte limit of the input queue is reached, packets are dropped.

Examples

The following example shows how to allow packets to be dropped when they have been queued for RBSCP tunnel encapsulation too long:

```
Router(config
)
# interface tunnel 0
Router(config
-if)#
 tunnel rbscp long_drop
```

Related Commands

Command	Description
show rbscp	Displays state and statistical information about RBSCP tunnels.
tunnel rbscp input_drop	Configures the input queue size on an RBSCP tunnel.

tunnel rbscp report

To report dropped Rate Based Satellite Control Protocol (RBSCP) packets to the Stream Control Transmission Protocol (SCTP), use the **tunnelrbscpreport** command in interface configuration mode. To disable dropped-packet reporting to SCTP, use the **no** form of this command.

tunnel rbscp report
no tunnel rbscp report

Syntax Description

This command has no arguments or keywords.

Command Default

RBSCP dropped-packet reporting is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

Use the **tunnelrbscpreport** command to provide early reporting of dropped RBSCP packets to SCTP instead of attempting retransmission of the packets at the router. SCTP will inform the end hosts of the dropped packets and allow the end hosts to retransmit the packets. Reporting dropped packets through SCTP provides better throughput because the packet dropping is not assumed to be caused by congestion.

Examples

The following example shows how to disable the SCTP drop reporting (reporting is enabled by default):

```
Router(config
)
# interface tunnel 0
Router(config
-if)#
 no tunnel rbscp report
```

Related Commands

Command	Description
show rbscp	Displays state and statistical information about RBSCP tunnels.

tunnel rbscp window_stuff

To enable TCP window stuffing by increasing the value of the TCP window scale for Rate Based Satellite Control Protocol (RBSCP) tunnels, use the **tunnelrbscpwindow_stuff** command in interface configuration mode. To restore the default TCP window scale value, use the **no** form of this command.

tunnel rbscp window_stuff *step-size*
no tunnel rbscp window_stuff

Syntax Description

step-size	Increment step size for the TCP window scale. Range is from 1 to 20. Default is 1.

Command Default

TCP window stuffing is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

Use the **tunnelrbscpwindow_stuff** command to make the sending host believe that the receiving host has a larger window by artificially increasing the TCP window size. RBSCP buffers the additional window and which be configured up to the satellite link bandwidth or the memory available on the router.

Note The actual TCP window size value that is used by the router may be smaller than the configured value because of the available bandwidth.

Examples

The following example shows how to enable TCP window stuffing on the RBSCP tunnel and configure a window size of 2:

```
Router(config
)
# interface tunnel 0
Router(config
-if)#
 tunnel rbscp window_stuff 2
```

Related Commands

Command	Description
show rbscp	Displays state and statistical information about RBSCP tunnels.

tunnel route-via

To specify the outgoing interface of the tunnel transport, use the **tunnelroute-via** command in interface configuration mode. To disable the source address selection, use the **no** form of this command.

tunnel route-via *interface-type interface-number* {**mandatory** | **preferred**}
no tunnel route-via

Syntax Description

interface-type	Indicates the type of interface.
interface-number	Indicates the interface number of the interface configured as the tunnel transport.
mandatory	Drops the traffic if the route is not available.
preferred	If the route is not available, forwards the traffic using any available route.

Command Default

This command is disabled by default. The tunnel transport cannot be routed using a subset of the routing table.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

If the **tunnelroute-via***interface-typeinterface-number***mandatory** command is configured, and there is no route to the tunnel destination using that interface, a point-to-point tunnel interface will go into a down state.

Examples

The following example shows the options that are available to configure the interfaces of the tunnel transport and route the tunnel transport using a subset of the routing table:

```
Router> enable
Router# configure terminal
Router(config)# interface tunnel 0
Router(config-if)# tunnel route-via ethernet0 mandatory
```

Related Commands

Command	Description
debug tunnel route-via	Displays information about the source address selection.
show interfaces tunnel	Displays information about the physical output tunnel interface.

tunnel sequence-datagrams

To configure a tunnel interface to drop datagrams that arrive out of order, use the **tunnelsequence-datagrams** command in interface configuration mode. To disable this function, use the **no** form of this command.

tunnel sequence-datagrams
no tunnel sequence-datagrams

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command currently applies to generic routing encapsulation (GRE) only. This command is useful when carrying passenger protocols that behave poorly when they receive packets out of order (for example, LLC2-based protocols).

Examples

The following example shows how to configure the tunnel to drop datagrams that arrive out of order:

```
Router(config
-if)
# tunnel sequence-datagrams
```

tunnel source

To set the source address for a tunnel interface, use the **tunnel source** command in interface configuration mode. To remove the source address, use the **no** form of this command.

tunnel source {*ip-addressipv6-address* | *interface-type interface-number* | **dynamic**}
no tunnel source

Command Syntax for Cisco Catalyst 3850 Series Switches

tunnel source *ip-address*
no tunnel source

Syntax Description

dynamic	Applies the tunnel source address dynamically to the tunnel interface.
ip-address	Source IP address of packets in the tunnel. • In case of traffic engineering (TE) tunnels, the control packets are affected.
ipv6-address	Source IPv6 address of packets in the tunnel.
interface-type	Interface type.
interface-number	Port, connector, or interface card number. The numbers are assigned at the factory at the time of installation or when added to a system and can be displayed with the **show interfaces** command.

Command Default

No tunnel interface source address is set.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
12.3(7)T	The address field has been updated to accept an IPv6 address as the source address allowing an IPv6 node to be used as a tunnel source.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS Release 2.1 and implemented on Cisco ASR 1000 Series Aggregation Services Routers.

Release	Modification
15.1SY	This command was integrated into Cisco IOS Release 15.1SY.
Cisco IOS XE Release 3.7S	This command was modified. The **dynamic** keyword was added.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

The source address is either an explicitly defined IP address or the IP address assigned to the specified interface.

You cannot have two tunnels using the same encapsulation mode with exactly the same source and destination addresses. The workaround is to create a loopback interface and source packets from the loopback interface. This restriction is applicable only for generic routing encapsulation (GRE) tunnels. You can have more than one TE tunnel with the same source and destination addresses.

Note **Only GRE tunneling is supported on Cisco Catalyst 3850 Series Switches.**

When using tunnels to Cayman boxes, you must set the **tunnel source** command to an explicit IP address on the same subnet as the Cayman box, and not the tunnel itself.

GRE tunnel encapsulation and deencapsulation for multicast packets are handled by the hardware. Each hardware-assisted tunnel must have a unique source. Hardware-assisted tunnels cannot share a source even if the destinations are different. You should use secondary addresses on loopback interfaces or create multiple loopback interfaces to ensure that the hardware-assisted tunnels do not share a source.

Cayman Tunnel Example

The following example shows how to set a tunnel source address for Cayman tunneling:

```
Device(config)# interface tunnel0
Device(config-if)# tunnel source ethernet0
Device(config-if)# tunnel destination 172.32.164.19
Device(config-if)# tunnel mode cisco1
```

Dynamic Tunnel Example

The following example shows how to set the tunnel source dynamically:

```
Device(config)# interface tunnel0
Device(config-if)# tunnel source dynamic
Device(config-if)# *Nov 22 19:38:28.271: Tunnel notified source change: dynamic is set
Device(config-if)# end
Device# show run interface tunnel0
Building configuration...

Current configuration : 63 bytes
!
interface Tunnel0
 no ip address
 tunnel source dynamic
end
```

If the tunnel source is configured to be set dynamically, you cannot configure the tunnel source address without removing the dynamic configuration.

```
Device(config)# interface tunnel0
Device(config-if)# tunnel source ethernet 0/0
Device(config-if)# *Nov 22 21:39:52.423: Tunnel notified source change: dynamic is set
*Nov 22 21:39:52.423: Tunnel notified source change, src ip 1.1.1.1
Device(config-if)# end
Device# show run interface tunnel0
Building configuration...

Current configuration : 63 bytes
!
interface Tunnel0
 no ip address
 tunnel source dynamic
end
Device# configure terminal
Device(config)# interface tunnel0
Device(config-if)# no tunnel source
Device(config-if)# *Nov 22 21:41:10.287: Tunnel notified source change: dynamic is not set
```

GRE Tunneling Example

The following example shows how to set a tunnel source address for GRE tunneling:

```
Device(config)# interface tunnel0
Device(config-if)# appletalk cable-range 4160-4160 4160.19
Device(config-if)# appletalk zone Engineering
Device(config-if)# tunnel source ethernet0
Device(config-if)# tunnel destination 172.32.164.19
Device(config-if)# tunnel mode gre ip
```

GRE Tunneling Examples for Cisco Catalyst 3850 Series Switches

The following example shows how to configure the logical Layer 3 GRE tunnel interface tunnel 2 in Global or non- VRF environment on Cisco Catalyst 3850 Series Switches:

```
Device(config)# interface tunnel 2
Device(config-if)# ip address 100.1.1.1 255.255.255.0
Device(config-if)# tunnel source 10.10.10.1
Device(config-if)# tunnel destination 10.10.10.2
Device(config-if)# tunnel mode gre ip
Device(config-if)# end
```

The following example shows how to configure the logical Layer 3 GRE tunnel interface tunnel 2 in VRF environment on Cisco Catalyst 3850 Series Switches. Use the **vrf definition** *vrf-name* and the**vrf forwarding** *vrf-name* commands to configure and apply VRF.

```
Device(config)# vrf definition RED
Device(config-vrf)#  address-family ipv4
Device(config-vrf-af)# exit-address-family
Device(config-vrf)#  exit
Device(config)# interface tunnel 2
Device(config)# vrf forwarding RED
Device(config-if)# ip address 100.1.1.1 255.255.255.0
Device(config-if)# tunnel source 10.10.10.1
Device(config-if)# tunnel destination 10.10.10.2
```

```
Device(config-if)# tunnel mode gre ip
Device(config-if)# end
```

Note **IPv6 GRE tunneling is not supported on Cisco Catalyst 3850 Series Switches.**

MPLS TE Tunnel Example

The following example shows how to set a tunnel source for a Multiprotocol Label Switching (MPLS) TE tunnel:

```
Device> enable
Device# configure terminal
Device(config)# interface tunnel 1
Device(config-if)# ip unnumbered loopback0
Device(config-if)# tunnel source loopback1
Device(config-if)# tunnel mode mpls traffic-eng
Device(config-if)# end
```

Related Commands

Command	Description
appletalk cable-range	Enables an extended AppleTalk network.
appletalk zone	Sets the zone name for the connected AppleTalk network.
tunnel destination	Specifies the destination for a tunnel interface.

tunnel tos

To configure the type of service (ToS) byte value for a tunnel interface, use the **tunneltos** command in interface configuration mode. To use the payload ToS byte value (if payload protocol is IP) or 0, use the **no** form of this command.

tunnel tos *tos-bytes*
no tunnel tos

Syntax Description

tos-bytes	ToS byte value from 0 to 255 specified in the encapsulating IP header of a tunneled packet. The default value is 0.

Command Default

The default ToS byte value is the payload ToS byte value (if payload protocol is IP); otherwise, 0.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(17)S	This command was introduced.
12.0(17)ST	This command was integrated into Cisco IOS Release 12.0(17)ST.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If the **tunneltos** command is not configured and the packet to be encapsulated is not an IP packet, the tunnel interface will use a default value of 0. If the **tunneltos**command is not configured and the packet to be encapsulated is an IP packet, the tunnel interface will use the ToS byte value of the inner IP packet header.

Examples

The following example shows how to configure a ToS byte value of 55 on tunnel interface 1:

```
interface tunnel 1
 tunnel tos 55
```

Related Commands

Command	Description
show interfaces tunnel	Lists tunnel interface information.
tunnel ttl	Configures the TTL hop-count value for a tunnel interface.

tunnel ttl

To configure the Time-to-Live (TTL) hop-count value for a tunnel interface, use the **tunnelttl** command in interface configuration command. To use the payload TTL value (if payload protocol is IP) or 255, use the **no** form of this command.

tunnel destination commandtunnel ttl *hop-count*
no tunnel ttl

Syntax Description

hop-count	TTL hop-count value from 1 to 255 to be used in the encapsulating IP header of a tunneled packet. The default is 255.

Command Default

The TTL default hop-count value is 255.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(17)S	This command was introduced.
12.0(17)ST	This command was integrated into Cisco IOS Release 12.0(17)ST.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to configure a TTL hop-count value of 200 on tunnel interface 1:

```
interface tunnel 1
 tunnel ttl 200
```

Related Commands

Command	Description
show interfaces tunnel	Lists tunnel interface information.
tunnel tos	Configures the ToS byte value for a tunnel interface.

tunnel vrf

To associate a VPN routing and forwarding (VRF) instance with a specific tunnel destination, interface, or subinterface, use the **tunnel vrf** command in global configuration or interface configuration mode. To disassociate a VRF from the tunnel destination, interface, or subinterface, use the **no** form of this command.

tunnel vrf *vrf-name*
no tunnel vrf *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF.

Command Default

The default destination is determined by the global routing table.

Command Modes

Global configuration (config)

Interface configuration (config-if)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA. Support was added for the Cisco 10000 Series Routers.
12.2(31)SB5	This command was integrated into Cisco IOS Release 12.2(31)SB5.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Usage Guidelines

To associate a VRF instance with a specific tunnel destination, ensure that the tunnel source and destination are in the same VRF.

Use the **ip vrf forwarding** command to associate a VRF instance with an interface or a subinterface other than a tunnel interface.

Use the **no ip vrf forwarding** *vrf-name* command or the **no tunnel vrf** *vrf-name* command to set either the IP VRF or the tunnel VRF to the global routing table.

The tunnel is disabled if no route to the tunnel destination is defined. If the tunnel VRF is set, you must configure a route to that destination in the VRF.

Cisco 10000 Series Routers and Cisco ASR 1000 Series Aggregation Services Routers

The VRF associated with the tunnel through the **tunnel vrf** command is the same as the VRF associated with the physical interface over which the tunnel sends packets (outer IP packet routing).

Examples

The following example shows how to associate a VRF with a tunnel destination. The tunnel endpoint 10.5.5.5 is looked up in the VRF named vrf2.

```
Device(config)# interface tunnel0
Device(config-if)# ip vrf forwarding vrf1
Device(config-if)# ip address 10.3.3.3 255.255.255.0
Device(config-if)# tunnel source loop 0
Device(config-if)# tunnel destination 10.5.5.5
Device(config-if)# tunnel vrf vrf2
```

Related Commands

Command	Description
ip route vrf	Establishes static routes for a VRF.
ip vrf	Configures a VRF routing table.
ip vrf forwarding	Associates a VRF instance with an interface or subinterface.
tunnel destination	Specifies the destination for a tunnel interface.
tunnel source	Sets the source address for a tunnel interface.

type STS48c

Use this command to configure protection group type.

type STS48c

There are no keywords for this command.

Command Default

None

Command Modes

Controller configuration

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1	Support for this command was introduced for the Cisco NCS 4200 Series and Cisco ASR 900 Series Routers.

Examples

The following example shows how to configure protection group:

```
enable
configure terminal
protection-group 401 type STS48c
controller protection group 401
type STS48c
cem-group 19001 cep
end
```

Related Commands

Command	Description
show protection-group	Verifies the protection group configuration.

tx-queue-limit

To control the number of transmit buffers available to a specified interface on the multiport communications interface (MCI) and serial communications interface (SCI) cards, use the **tx-queue-limit** command in interface configuration mode.

tx-queue-limit *number*

Syntax Description

number	Maximum number of transmit buffers that the specified interface can subscribe.

Command Default

Defaults depend on the total transmit buffer pool size and the traffic patterns of all the interfaces on the card. Defaults and specified limits are displayed with the **showcontrollersmci** command.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command should be used only under the guidance of a technical support representative.

This command does not have a **no** form.

Examples

The following example shows how to set the maximum number of transmit buffers on the interface to 5:

```
Router
(config)
# interface ethernet 0
Router
(config-if)
# tx-queue-limit 5
```

Related Commands

Command	Description
show controllers mci	Displays all information under the MCI card or the SCI.

ucse subslot imc password-reset

To reset the Cisco Integrated Management Controller (CIMC) password, use the **ucse subslot imc password-reset** command in privileged EXEC mode.

ucse subslot *slot/subslot* **imc password-reset**

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the NIM E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot number is 0.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced on the Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Router (ISR).
Cisco IOS XE Release 3.15S	This command was supported on an additional platform: the NIM E-Series Network Compute Engine (NIM E-Series NCE) installed in a Cisco ISR 4000 Series.

Usage Guidelines

After you enter this command, at the next login, the system requests that you set a new password to access CIMC.

Examples

The following example shows how to reset the CIMC password in an E-Series Server installed in a Cisco ISR 4000 series:

```
Router# ucse subslot 1/0 imc password-reset
Router#
 IMC ACK: UCSE password reset successful for IMC
```

ucse subslot server

To reload, reset, start, or stop the hardware on the server module, use the **ucse subslot server** command in privileged EXEC mode.

ucse subslot *slot/subslot* **server** {**reload** | **reset** | **start** | **stop**}

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the NIM E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot number is 0.
reload	Powers down the server module and then powers it on. **Note** The **reload** keyword is not supported on the NIM E-Series-NCE. Instead, we recommend that you use the following commands from the router: 1. Router # **ucse subslot** *slot/subslot* **shutdown** 2. Router # **ucse subslot** *slot/subslot* **start** If a reload is necessary, use the following command: Router # **hw-module subslot 0/***NIM-slot-number* **reload** **Note** This command power-cycles the module. The CIMC and server reboot.
reset	Resets the hardware on the server module.
start	Powers on the server module.
stop	Immediately powers down the server module. **Note** The **stop** keyword is not supported on the NIM E-Series-NCE. Instead, we recommend that you use the following command from the router: Router # **ucse subslot** *slot/subslot* **shutdown** If it is necessary to do an immediate power down of the server, use the following command: Router # **hw-module subslot 0/***NIM-slot-number* **stop** **Note** This command powers down the module. The CIMC and server power off.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced on the Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Router (ISR).
Cisco IOS XE Release 3.15S	This command was supported on an additional platform: the NIM E-Series Network Compute Engine (NIM E-Series NCE) installed in a Cisco ISR 4000 Series.

Usage Guidelines

Use the **reset** keyword only to recover from a shutdown or failed state.

Caution Using the **reset** keyword does *not* provide an orderly software shutdown and may impact file operations that are in progress.

Examples

The following example shows how to reload the E-Series Server installed in a Cisco ISR 4000 series:

```
Router# ucse subslot 1/0 server reload
Router#
 IMC ACK: UCSE Server reload successful.
```

The following example shows how to reset the E-Series Server installed in a Cisco ISR 4000 series:

```
Router# ucse subslot 1/0 server reset
Router#
 IMC ACK: UCSE Server reset successful.
```

The following example shows how to start the E-Series Server installed in a Cisco ISR 4000 series:

```
Router# ucse subslot 1/0 server start
Router#
 IMC ACK: UCSE Server start successful.
```

The following example shows how to stop the E-Series Server installed in a Cisco ISR 4000 series:

```
Router# ucse subslot 1/0 server stop
Router#
 IMC ACK: UCSE Server stop successful.
```

ucse subslot server password-reset

To reset the BIOS or RAID password, use the **ucse subslot server password-reset** command in privileged EXEC mode.

ucse subslot *slot/subslot* **server password-reset** {**BIOS** | **RAID**}

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the NIM E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot number is 0.
BIOS	Resets the BIOS password.
RAID	Resets the RAID password. **Note** RAID is not supported on the NIM E-Series NCE.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced on the Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Router (ISR).
Cisco IOS XE Release 3.15S	This command was supported on an additional platform: the NIM E-Series Network Compute Engine (NIM E-Series NCE) installed in a Cisco ISR 4000 Series.

Usage Guidelines

After you enter this command, at the next login, the system requests that you set a new password to access BIOS or configure RAID.

Examples

The following example shows how to reset the BIOS password in an E-Series Server installed in a Cisco ISR 4000 series:

```
Router# ucse subslot 1/0 server password-reset BIOS
Router#
 IMC ACK: UCSE password reset successful for BIOS
```

The following example shows how to reset the RAID password in an E-Series Server installed in a Cisco ISR 4000 series:

```
Router# ucse subslot 1/0 server password-reset RAID
```

```
Router#
 IMC ACK: UCSE password reset successful for RAID
```

ucse subslot shutdown

To gracefully shut down the server module, use the **ucse subslot shutdown** command in privileged EXEC mode.

ucse subslot *slot/subslot* **shutdown**

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the NIM E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot number is 0.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced on the Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Router (ISR).
Cisco IOS XE Release 3.15S	This command was supported on an additional platform: the NIM E-Series Network Compute Engine (NIM E-Series NCE) installed in a Cisco ISR 4000 Series.

Usage Guidelines

The NIM E-Series NCE might take up to 60 seconds to shut down. After two or three shut down attempts, if the NIM E-Series NCE does not shut down, enter the following commands from the router:

1. Router # **hw-module subslot 0/***NIM-slot-number* **stop**
2. Router # **hw-module subslot 0/***NIM-slot-number* **start**

Examples

The following example shows how to shut down an E-Series Server installed in a Cisco ISR 4000 series:

```
Router# ucse subslot 1/0 shutdown
Router#
 IMC ACK: UCSE Server shutdown successful.
```

ucse subslot statistics

To display or clear server module statistics, use the **ucse subslot statistics** command in privileged EXEC mode.

ucse subslot *slot/subslot* **statistics** [**clear**]

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the NIM E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot number is 0.
clear	(Optional) Clears the server module statistics.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced on the Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Router (ISR).
Cisco IOS XE Release 3.15S	This command was supported on an additional platform: the NIM E-Series Network Compute Engine (NIM E-Series NCE) installed in a Cisco ISR 4000 Series.

Examples

The following example shows how to display the statistics of an E-Series Server:

```
Router# ucse subslot 1/0 statistics
 Count of number of shutdowns command : 1
 Count of number of status commands : 0
 Count of number of server raid password  : 1
 Count of number of imc password-reset : 2
 Count of number of server bios password reset : 1
 Count of number of server reload : 1
 Count of number of server reset : 1
 Count of number of server start : 1
 Count of number of server stop : 1
 Count of number of vlan commands : 0
 Count of number of access-port commands : 1
 Count of number of IMC configured IP or DHCP commands: 1
```

ucse subslot status

To display configuration information related to the hardware and software on the server module, use the **ucse subslot status** command in privileged EXEC mode.

ucse subslot *slot/subslot* **status** [**detailed**]

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the NIM E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot number is 0.
detailed	(Optional) Displays detailed information about the server module, such as its status and settings of the reset and heartbeat-reset flags.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced on the Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Router (ISR).
Cisco IOS XE Release 3.15S	This command was supported on an additional platform: the NIM E-Series Network Compute Engine (NIM E-Series NCE) installed in a Cisco ISR 4000 Series.

Examples

The following example shows how to display the status of an E-Series Server:

```
Router#  ucse subslot 1/0 status
CPU info
        Name         Cores    Version
        ------------ -------- --------------------------------------------------
        CPU1         4        Intel(R) Xeon(R) CPU E5-2418L 0 @ 2.00GHz

Memory info
        Name                 Capacity        Channel Speed (MHz) Channel Type
        -------------------- --------------- ------------------- ---------------
        Node0_Dimm0          Not Installed   Unknown             Unknown
        Node0_Dimm1          16384 MB        1333                DDR3
        Node0_Dimm2          8192 MB         1333                DDR3

Hard drive info
        Slot Number Controller Status                Manufacturer   Model          Drive
Firmware Coerced Size   Type  SED
        ----------- ---------- --------------------- -------------- --------------
-------------- -------------- ----- -----
        1           SLOT-5     online                ATA            ST91000640NS   CC02
```

```
         952720 MB      HDD   false
        2           SLOT-5     online                 ATA           ST91000640NS   CC02
         952720 MB      HDD   false
        3           SLOT-5     online                 ATA           ST91000640NS   CC02
         952720 MB      HDD   false

Virtual drive info
        Virtual Drive  Status               Name                     Size       RAID Level

        -------------- -------------------- ------------------------ ---------- ----------

        0              Optimal                                       1905440 MB RAID 5


PCI card info
        Name                 Slot       Vendor ID            Device ID            Product
Name
        -------------------- ---------- -------------------- --------------------
-------------------------
        PCIe Adapter1        0          0xe414               0x5716               Broadcom
 5719 1 Gbps 4...
       PCIe Adapter2        2          0x0010               0x7300              LSI 9240-8i
 MegaRAID S...

Network Setting
            IPv4 Address: 10.1.1.2
            IPv4 Netmask: 255.255.255.0
            IPv4 Gateway: 10.1.1.1

            NIC Mode: shared_lom
            NIC Redundancy: none
            NIC Interface: ge1
```

ucse cmos-reset

To reset the BIOS CMOS, use the **ucse cmos-reset** command in privileged EXEC mode.

E-Series Servers Installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T

ucse *slot* **cmos-reset**

E-Series Servers and EHWIC E-Series NCE Installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M

ucse subslot *slot/subslot* **cmos-reset**

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the EHWIC E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot number is 0.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(4)M	This command was introduced. This command was supported on Cisco UCS E-Series Servers (E-Series Server) installed in an ISR G2.
15.4(3)M	This command was modified to include the **subslot** keyword. This command was supported on an additional platform: the EHWIC E-Series Network Compute Engine (EHWIC E-Series NCE) installed in an ISR G2.

Usage Guidelines

This command sets the BIOS CMOS back to the factory defaults. User changes made in the BIOS will be lost.

Examples

The following example shows how to reset the BIOS CMOS in an E-Series Server installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T:

```
Router# ucse 2 cmos-reset
```

Examples

The following example shows how to reset the BIOS CMOS in an E-Series Server or EHWIC E-Series NCE installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M:

```
Router# ucse subslot 0/3 cmos-reset
```

ucse heartbeat-reset

To enable or disable Cisco IOS software from rebooting the Cisco E-Series Server when the heartbeat is lost, use the **ucse heartbeat-reset** command in EXEC mode.

ucse *slot* **heartbeat-reset** [{**disable** | **enable**}]

Syntax Description

slot	Router slot number in which the Cisco E-Series Server is installed.
enable	Does not allow the Cisco IOS software to reboot the Cisco E-Series Server when the heartbeat is lost.
disable	Allows the Cisco IOS software to reboot the Cisco E-Series Server when the heartbeat is lost.

Command Modes

Privileged EXEC mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to reset the slot server heartbeat:

```
Router# ucse 2 heartbeat-reset enable
```

ucse imc config

To save the CIMC configuration to a file on the router’s flash drive or to restore the CIMC configuration from a file on the router’s flash drive, use the **ucse imc config** command in EXEC mode.

ucse *slot* **imc config** {**restore** | **save**} **url**

Syntax Description

slot	Router slot number in which the Cisco E-Series Server is installed.
restore	Restores the CIMC configuration from a file.
save	Saves the CIMC configuration to a file.
url	The url where the configuration file is located.

Command Modes

Privileged EXEC mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

Itis important to store the CIMC configuration to a file in case you need to move the HDDs from one module to another.

Examples

The following example shows how to save the CIMC configuration to a file:

```
Router# ucse 2 imc config save flash0:my-imc-config
```

ucse imc file delete

To delete the CIMC image file, use the **ucse imc file delete** command in EXEC mode. The file can be either a .iso or .img file.

ucse *slot* **imc** **file** **delete** *file_name*

Syntax Description

slot	Router slot number in which the Cisco E-Series Server is installed.
file_name	Name of the CIMC image file to delete. **Note** The name of the file must match exactly the name of the file as displayed by the output of the **show** **ucse** *slot* **imc files**command.

Command Modes

Privileged EXEC mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

You can only delete one file at a time.

Examples

The following example shows how to delete the CIMC image file:

```
Router# ucse 2 imc file delete xxxxx.iso

Delete the IMC file xxxxx.iso [confirm]
Deleted
```

ucse imc file download

To download the CIMC image file in the background to an internal storage device, use the **ucse imc file download** command in EXEC mode. The file must have a .iso file extension.

ucse *slot* **imc file download** {**URL** *url* | **abort**}

Syntax Description

slot	Router slot number in which the Cisco E-Series Server is installed.
url	Downloads the CIMC image file from the specified HTTP, HTTPS, SFTP, or FTPS server.
abort	Aborts the downloading of the file.

Command Modes

Privileged EXEC mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

You can only download one file at a time.

To check the download progress after initiating a download, issue the **show ucse** *slot* **imc download progress** command.

Examples

The following example shows how to download the CIMC image file:

```
Router# ucse 2 imc file download URL http://xxxxx.iso
Started downloading file from http://xxxxx.iso

Router# show ucse 2 imc file download progress
Downloaded 23%
```

The following example shows how to abort a download of the CIMC image file:

```
Router# ucse 2 imc file download abort

Abort the IMC file download? [confirm] y
Download aborted.
```

ucse password-reset

To reset the BIOS, CIMC, or RAID password, use the **ucse password-reset** command in privileged EXEC mode.

E-Series Servers Installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T

ucse *slot* **password-reset** {**BIOS** | **BMC** | **RAID**}

E-Series Servers and EHWIC E-Series NCE Installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M

ucse **subslot** *slot/subslot* **password-reset** {**BIOS** | **BMC** | **RAID**}

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the EHWIC E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot number is 0.
BIOS	Resets the BIOS password.
BMC	Resets the CIMC password.
RAID	Resets the RAID password. **Note** RAID is not applicable for the EHWIC E-Series Network Compute Engine (EHWIC E-Series NCE).

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(4)M	This command was introduced. This command was supported on Cisco UCS E-Series Servers (E-Series Server) installed in an ISR G2.
15.4(3)M	This command was modified to include the **subslot** keyword. This command was supported on an additional platform: the EHWIC E-Series NCE installed in an ISR G2.

Usage Guidelines

After this command has been entered, the system requests that a new password be set when accessing the BIOS or BMC.

RAID is not applicable for the EHWIC E-Series NCE.

Examples

The following example shows how to reset the BIOS password in an E-Series Server installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T:

```
Router# ucse 2 password-reset BIOS

Reset command sent
```

Examples

The following example shows how to reset the BIOS password in an E-Series Server or EHWIC E-Series NCE installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M:

```
Router# ucse subslot 0/3 password-reset BIOS

Reset command sent
```

ucse server boot

To reload, reset, or boot the Cisco E-Series Server from a particular URL, use the **ucse server boot** command in EXEC mode.

ucse *slot* **server** {**reload** | **reset** | **start**} **boot** {**url** *url* | **device** *device_type*} [**argument** *text*]

Syntax Description

slot	Router slot number in which the Cisco E-Series Server is installed.
url *url*	Boots the Cisco E-Series Server from an externally stored file, which can be either a .iso or .img file. The URL can be one of the following types: • HTTP • FTP • SFTP • FTPS://XXXXX.iso Restrictions: • This argument accepts IPv6 and IPv4 addresses, as well as literal names. • The name of the file must match exactly the name of the file as displayed by the output of the **show ucse** *slot* **imc file**command.
device *device_type*	The device type from which the E-Series Server boots. It can be one of the following: • HDD:*device_name* —Hard disk drive • FDD—Floppy disk drive • CDROM:*device_name* —Bootable CD-ROM • PXE—PXE boot • EFI—Extensible Firmware Interface **Note** The name of the devices must match exactly the names as displayed by the output of the **show ucse** *slot* **server boot devices**command.
argument *text*	An arbitrary text string.

Command Modes

Privileged EXEC mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

This command works by first downloading the specified file to local storage, reloading the server from that file, and then booting the installed system.

After issuing this command, the system modifies the boot order so that the downloaded image is first.

After you have issued this command with the **url** argument and keyword, use the **show** *ucse* **slot server boot progress**command to see the results.

After you have issued this command with the **device** argument and keyword, use the **show** *ucse* **slot server boot order**command to see the results.

Examples

The following example shows how to boot the server from a URL:

```
Router# ucse 2 server reload boot url http://path/to/iso
Router# show ucse 2 server boot progress

Downloading http://path/to/iso 44%
```

The following example shows how to boot the server from an HDD:

```
Router# ucse 2 server reset boot device HDD
Router# show ucse 2 server boot progress

System started
```

The following example shows how to start the server from an HDD:

```
Router# ucse 2 server start boot device HDD
Router# show ucse 2 server boot progress
```

ucse server boot order

To configure the boot order for the Cisco E-Series Server, use the **ucse server boot order** command in EXEC mode.

ucse *slot* **server boot order device_1** [**device_2**] [**device_3**] [**device_4**]

Syntax Description

slot	Router slot number in which the Cisco E-Series Server is installed.
device_1 device_2 device_3 device_4	Specifies the devices to boot. **Note** The name of the devices must match exactly the names as displayed by the output of the **show ucse** *slot* **server boot devices**command. The device can be any of the following, but you can only use each device name once when issuing this command: • PXE—PXE boot • FDD—Floppy disk drive • HDD:*device_name* —Hard disk drive • CDROM:*device_name* —Bootable CD-ROM

Command Modes

Privileged EXEC mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

Due to BIOS limitations, you can only specify each device type (PXE, FDD, HDD, and CDROM) once per group. Therefore, it is impossible to set up a boot order with two HDDs or two CDROMs.

To determine the devices available from which you can boot the server, issue the **show ucse** *slot* **server boot devices** command.

To check the boot order configuration after issuing this command, issue the **show ucse** *slot* **server boot order** command.

Examples

The following example shows how to configure the boot order:

```
Router# show ucse 2 server boot devices

PXE
FDD
HDD:HDD3
HDD:RAID-MD0
HDD:USB-FF5D6CC3DAA67F12-1
CDROM:USB-CD
Router# ucse 2 boot order PXE CDROM:USB-CD FDD HDD:RAID-MD0
```

```
Router# show ucse 2 server boot order
Currently booted from CDROM:USB-CD
Boot order:
1) PXE
2) CDROM:USB-CD
3) FDD
4) HDD:RAID-MD0
```

ucse server erase device hdd

To erase all existing data from the Cisco E-Series Server hard drive devices (HDDs), use the **ucse server erase device hdd** command in EXEC mode.

ucse *slot* **server erase device hdd** {**ALL** | **use** *device_list*}

Syntax Description

slot	Router slot number in which the Cisco E-Series Server is installed.
device_list	Erases the data from only the specified HDDs. **Note** The name of the devices must exactly match the names as displayed by the output of the **show ucse** *slot* **server boot devices**command.

Command Modes

Privileged EXEC mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

Use this command if you need to remove sensitive data from a hard drive before shipping the server. The system prompts you to confirm that you really want to erase the data from the hard drive device.

Caution Use this command with caution, as it erases the contents of the HDDs.

To check the status of the hard drive after you have issued this command, use the **show ucse** *slot* **server erase device status** command.

Examples

The following example shows how to erase the data from the device called HDD2, and then display the status:

```
Router# ucse 2 server erase device hdd use hdd2

You are about to erase all data on the selected hard drives.
Proceed with drive erasure? y

Erasing HDD2 started

Router# show ucse 2 server erase device status

HDD2 erased 0 %
```

ucse server raid level

To configure the RAID array on the Cisco E-Series Server, use the **ucse server raid level** command in EXEC mode.

ucse *slot* **server raid level** {**0** | **1** | **5** | **NONE** | **use** *device_list*}

Syntax Description

slot	Router slot number in which the Cisco E-Series Server is installed.
0	Data is stored evenly in stripe blocks across two or more disks without redundancy (mirroring).
1	Data is stored in mirrored set of disk drives with an optional hot spare disk drive.
5	Data is stored in stripe blocks with parity data staggered across all disk drives.
NONE	Disk drives of a computer are not configured as RAID and are put in a JBOD configuration.
use *device_list*	Allows you to configure more than one device at a time. If you do not use the **use** keyword, then the system configures all hard drives into a RAID in the order in which they are detected by the module. Enter the list of HDDs using a comma-separated list, such as HDD1, HDD2, HDD3. This command only applies to the internal HDDs, which are named according to their physical location. **Note** The name of the devices must match exactly the names as displayed by the output of the **show ucse** *slot* **server boot devices**command.

Command Modes

Privileged EXEC mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

This command only applies to HDDs.

Caution Use this command with caution, as it destroys the contents of the HDDs. Do not use this command to migrate the RAID configuration.

After you have issued this command, use the **show** *ucse* **slot server raid level**command to see the results.

Examples

The following example shows how to configure RAID level 1:

```
Router# ucse 2 server raid level 1

You are about to change RAID configuration.
This will destroy all data on the hard drives.
Proceed with setting new RAID level? [confirm] y
```

```
RAID reconfigured

Router# show ucse 2 server raid level

RAID 0 (Ctrl:SLOT-5 ID:0 Size:1905440 MB State:Optimal)
        HDD1 :              953869 MB online (0 errors)
        HDD255 :              953869 MB online (0 errors)

        HDDs not in the RAID:
        HDD2 :              286102 MB system (0 errors)
```

ucse server reload boot

To boot the Cisco E-Series Server from a particular url or device type, use the **ucse server reload boot** command in EXEC mode.

ucse *slot* **server reload boot** {**url** *url* | **device** *device_type*}

Syntax Description

slot	Router slot number in which the Cisco E-Series Server is installed.
url *url*	Boots the Cisco E-Series Server from the specified url.
device *device_type*	The device type from which the Cisco E-Series Server boots. It can be one of the following: • CDROM: Virtual-CD • EFI • FDD: Virtual-Floppy • HDD: RAID • HDD: SD2 • HDD: Virtual-HiFD • PXE: GIGETH0 • PXE: GIGETH1 • PXE: GIGETH3

Command Modes

Privileged EXEC mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

Use this command to safely reload the server.

Examples

The following example shows how to reload the server:

```
Router# ucse 2 server reload boot url http://220.0.0.100/OS/image.iso
```

ucse server reset boot

To reset the hardware on the Cisco E-Series Server, use the **ucse server reset boot** command in EXEC mode.

ucse *slot* **server reset boot** {**url** *url* | **device** *device_type*}

Syntax Description

slot	Router slot number in which the Cisco E-Series Server is installed.
url *url*	Boots the Cisco E-Series Server from the specified url.
device *device_type*	The device type from which the Cisco E-Series Server boots. It can be one of the following: • CDROM: Virtual-CD • EFI • FDD: Virtual-Floppy • HDD: RAID • HDD: SD2 • HDD: Virtual-HiFD • PXE: GIGETH0 • PXE: GIGETH1 • PXE: GIGETH3

Command Modes

Privileged EXEC mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

Use this command only to recover from a shutdown or failed state.

Caution Using this command does *not* provide an orderly software shutdown and may impact file operations that are in progress.

Examples

The following example shows how to reset the server:

```
Router# ucse 2 server reset boot url http://220.0.0.100/OS/image.iso
```

ucse session

To start or close a host or CIMC session, use the **ucse session** command in privileged EXEC mode.

E-Series Servers Installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T

ucse *slot* **session** {**imc** [**clear**] | **host** [**clear**]}

E-Series Servers and EHWIC E-Series NCE Installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M

ucse subslot *slot/subslot* **session** {**imc** [**clear**] | **host** [**clear**]}

Note The **ucse** *slot* **session imc** command will work only if you have configured a router-side IP address (for instance, ip unnumbered GigabitEthernet0/0) on the interface.

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the EHWIC E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot number is 0.
imc	Starts a session with CIMC.
imc clear	Closes the existing CIMC session.
host	Starts a session with the host Cisco E-Series Server.
host clear	Closes the host Cisco E-Series Server session.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(4)M	This command was introduced. This command was supported on Cisco UCS E-Series Servers (E-Series Server) installed in an ISR G2.
15.4(3)M	This command was modified to include the **subslot** keyword. This command was supported on an additional platform: the EHWIC E-Series Network Compute Engine (EHWIC E-Series NCE) installed in an ISR G2.

Usage Guidelines

The **imc clear** and **host clear** commands close the active session of the CIMC or the host. As a result, the system closes the sessions of any other users currently logged in.

Only one active session is allowed in the CIMC or host at any time. If you receive a “connection refused” message when sessioning in, close the current active session by entering the **imc clear** or **host clear** commands.

Examples

The following example shows how to clear the CIMC session in an E-Series Server installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T:

```
Router# ucse 2 session imc clear
```

Examples

The following example shows how to clear the CIMC session in an E-Series Server or EHWIC E-Series NCE installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M:

```
Router# ucse subslot 0/3 session imc clear
```

ucse shutdown

To shut down the system gracefully, use the **ucse shutdown** command in privileged EXEC mode.

E-Series Servers Installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T

ucse *slot* **shutdown**

E-Series Servers and EHWIC E-Series NCE Installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M

ucse subslot *slot/subslot* **shutdown**

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the EHWIC E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot number is 0.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(4)M	This command was introduced. This command was supported on Cisco UCS E-Series Servers (E-Series Server) installed in an ISR G2.
15.4(3)M	This command was modified to include the **subslot** keyword. This command was supported on an additional platform: the EHWIC E-Series Network Compute Engine (EHWIC E-Series NCE) installed in an ISR G2.

Usage Guidelines

Use this command when removing or replacing a hot-swappable module during online insertion and removal (OIR).

Examples

The following example shows how to gracefully shut down an E-Series Server installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T:

```
Router# ucse 2 shutdown
```

Examples

The following example shows how to gracefully shut down an E-Series Server or EHWIC E-Series NCE installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M:

```
Router# ucse subslot 0/3 shutdown
```

ucse server start boot

To power on the Cisco E-Series Server using the boot option, use the **ucse server start boot** command in EXEC mode .

ucse *slot* **server start boot** {**url** *url* | **device** *device_type*}

Syntax Description

slot	Router slot number in which the Cisco E-Series Server is installed.
url *url*	Boots the Cisco E-Series Server from the specified url.
device *device_type*	The device type from which the Cisco E-Series Server boots. It can be one of the following: • CDROM: Virtual-CD • EFI • FDD: Virtual-Floppy • HDD: RAID • HDD: SD2 • HDD: Virtual-HiFD • PXE: GIGETH0 • PXE: GIGETH1 • PXE: GIGETH3

Command Modes

Privileged EXEC mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

Use this command to power on the server that was previously turned off.

Examples

The following example shows how to start the Cisco E-Series Server using the boot option:

```
Router# ucse 2 server start boot url http://220.0.0.100/OS/image.iso
```

ucse statistics

To display or clear the reset and reload server information, use the **ucse statistics** command in privileged EXEC mode.

E-Series Servers Installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T

ucse *slot* **statistics** **[clear]**

E-Series Servers and EHWIC E-Series NCE Installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M

ucse **subslot** *slot*/*subslot* **statistics** **[clear]**

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the EHWIC E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot number is 0.
clear	(Optional) Clears the E-Series Server's reset and reload information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(4)M	This command was introduced. This command was supported on Cisco UCS E-Series Servers (E-Series Server) installed in an ISR G2.
15.4(3)M	This command was modified to include the **subslot** keyword. This command was supported on an additional platform: the EHWIC E-Series Network Compute Engine (EHWIC E-Series NCE) installed in an ISR G2.

Examples

The following example shows how to display the server statistics in an E-Series Server installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T:

```
Router# ucse 2 statistics

Module Reset Statistics:
  CLI reset count = 0
  CLI reload count = 0
  Registration request timeout reset count = 0
  Error recovery timeout reset count = 0
  Module registration count = 1
```

Examples

The following example shows how to display the server statistics in an E-Series Server or EHWIC E-Series NCE installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M:

```
Router# ucse subslot 0/3 statistics

Module Reset Statistics:
  CLI reset count = 0
  CLI reload count = 0
  Registration request timeout reset count = 0
  Error recovery timeout reset count = 0
  Module registration count = 1
```

ucse status

To display configuration information related to the hardware and software of a server, use the **ucse status** command in privileged EXEC mode.

E-Series Servers Installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T

ucse *slot* **status** [**detailed**]

E-Series Servers and EHWIC E-Series NCE Installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M

ucse **subslot** *slot/subslot* **status** [**detailed**]

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the EHWIC E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot number is 0.
detailed	(Optional) Displays detail information about the Cisco E-Series Server such as the status of the service module and settings of the reset and heartbeat-reset flags.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(4)M	This command was introduced. This command was supported on Cisco UCS E-Series Servers (E-Series Server) installed in an ISR G2.
15.4(3)M	This command was modified to include the **subslot** keyword. This command was supported on an additional platform: the EHWIC E-Series Network Compute Engine (EHWIC E-Series NCE) installed in an ISR G2.

Examples

The following example shows how to display server status in an E-Series Server installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T:

```
Router# ucse 2 status

Service Module is Cisco ucse 2/0
Service Module supports session via TTY line 131
Service Module is in Steady state
Service Module reset on error is disabled
Service Module heartbeat-reset is enabled
```

Examples

The following example shows how to display server status in an E-Series Server or EHWIC E-Series NCE installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M:

```
Router# ucse subslot 0/3 status

Service Module is Cisco ucse 0/3
Service Module supports session via TTY line 131
Service Module is in Steady state
Service Module reset on error is disabled
Service Module heartbeat-reset is enabled
```

ucse stop

To immediately power down the server, use the **ucse stop** command in privileged EXEC mode.

E-Series Servers Installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T

ucse *slot* **stop**

E-Series Servers and EHWIC E-Series NCE Installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M

ucse subslot *slot/subslot* **stop**

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the EHWIC E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot number is 0.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(4)M	This command was introduced. This command was supported on Cisco UCS E-Series Servers (E-Series Server) installed in an ISR G2.
15.4(3)M	This command was modified to include the **subslot** keyword. This command was supported on an additional platform: the EHWIC E-Series Network Compute Engine (EHWIC E-Series NCE) installed in an ISR G2.

Examples

The following example shows how to power down an E-Series Server installed in an ISR G2—Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T:

```
Router# ucse 2 stop

Send server stop command
```

Examples

The following example shows how to power down an E-Series Server or EHWIC E-Series NCE installed in an ISR G2—Applicable in Cisco IOS Release 15.4(3)M:

```
Router# ucse subslot 0/3 stop

Send server stop command
```

unidirectional

To configure the software-based UDE, use the **unidirectional** command in interface configuration mode. To remove the software-based UDE configuration, use the **no** form of this command.

unidirectional {**send-only** | **receive-only**}
no unidirectional

Syntax Description

send-only	Specifies that the unidirectional transceiver transmits traffic only.
receive-only	Specifies that the unidirectional transceiver receives traffic only.

Command Default

UDE is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

UDE is supported on the interfaces of these switching modules:

- WS-X6704-10GE 4-port 10-Gigabit Ethernet
- WS-X6816-GBIC 16-port Gigabit Ethernet
- WS-X6516A-GBIC 16-port Gigabit Ethernet
- WS-X6516-GBIC 16-port Gigabit Ethernet

You do not need to configure software-based UDE on ports where you implement hardware-based UDE.

If an interface is configured with Unidirectional Ethernet or has a receive-only transceiver, UDLD is operationally disabled. Use the **showudld** command to display the configured and operational states of this interface.

When you apply the UDE configuration to an interface, the following warning message is displayed:

```
Warning!
Enable port unidirectional mode will automatically disable port udld. You must manually
ensure that the unidirectional link does not create a spanning tree loop in the network.
Enable l3 port unidirectional mode will automatically disable ip routing on the port. You
must manually configure static ip route and arp entry in order to route ip traffic.
```

Examples

This example shows how to configure 10-Gigabit Ethernet port 1/1 as a UDE send-only port:

```
Router(config-if)# unidirectional send-only
Warning!
Enable port unidirectional mode will automatically disable port udld. You must manually
ensure that the unidirectional link does not create a spanning tree loop in the network.
```

```
Enable l3 port unidirectional mode will automatically disable ip routing on the port. You
must manually configure static ip route and arp entry in order to route ip traffic.
```

This example shows how to configure 10-Gigabit Ethernet port 1/2 as a UDE receive-only port:

```
Router(config-if)# unidirectional receive-only
Warning!
Enable port unidirectional mode will automatically disable port udld. You must manually
ensure that the unidirectional link does not create a spanning tree loop in the network.
Enable l3 port unidirectional mode will automatically disable ip routing on the port. You
must manually configure static ip route and arp entry in order to route ip traffic.
```

Related Commands

Command	Description
show interfaces status	Displays the interface status or a list of interfaces in an error-disabled state on LAN ports only.
show interfaces unidirectional	Displays the operational state of an interface with a receive-only transceiver.

upgrade fpd auto

To configure the router to automatically upgrade the current FPD images on a SPA or any FPD-capable cards when an FPD version incompatibly is detected, enter the **upgradefpdauto** global configuration command. To disable automatic FPD image upgrades, use the **no** form of this command.

upgrade fpd auto
no upgrade fpd auto

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled by default if your router has any installed SPAs or FPD-capable cards. The router checks the FPD image during bootup or after an insertion of a SPA or FPD-capable card. If the router detects an incompatibility between an FPD image and a SPA or FPD-capable card, an automatic FPD upgrade attempt occurs unless the user has disabled automatic FPD upgrades by entering the **noupgradefpdauto** command. The **upgradefpdpath** command can be used to direct the router to search for the FPD image package at another location (such as an FTP or TFTP server) when an FPD incompatibility is detected.

The router searches the disk2: Flash Disk for the FPD image package file when an FPD incompatibility is detected and **upgradefpdauto** is enabled.

The **routersearchesthe**primary Flash file system (disk0:) for the FPD image package file when an FPD incompatibility is detected and **upgradefpdauto** is enabled.

The router searches all of its Flash file systems for the FPD image package when an FPD incompatibility is detected and **upgradefpdauto** is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(20)S2	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(4)XD3	This command was integrated into Cisco IOS Release 12.4(4)XD3.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

This command is enabled by default. In most cases, this default configuration should be retained.

If this command is disabled but an FPD upgrade is required for a SPA, the**upgradehw-modulesubslot** command can be used to upgrade the SPA FPD image manually after the SPA is disabled because of the existing FPD incompatibility.

If this command is disabled but an FPD upgrade is required for an FPD-capable card on the Cisco 7200 VXR router, you cannot upgrade the card manually. Select the FPD image package and download it to the disk2: Flash Disk, enable the automatic FPD upgrade by using the upgrade fpd auto command, and reboot the router.

Upgrading the FPD image on a SPA or FPD-capable card places the SPA or card offline while the upgrade is taking place. The time required to complete an FPD image upgrade can be lengthy. The **showupgradefpdprogress** command can be used to gather more information about estimated FPD download times for a particular SPA.

For more information about FPD upgrades on SPA interface processors (SIPs) and shared port adapters (SPAs), refer to the Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide.

Examples

Cisco 7200 VXR

The following example shows the output that is displayed when a VSA in slot 0 requires an FPD image upgrade and the upgrade fpd auto command is enabled. The required FPD image is automatically upgraded.

```
*Apr 10 00:37:42.859: %FPD_MGMT-3-INCOMP_IMG_VER: Incompatible VSA (FPD ID=1) image version
 detected for VSA card in slot 0. Detected version = 0.9, minimum required version = 0.10.
 Current HW version = 0.0.
*Apr 10 00:37:42.859: %FPD_MGMT-5-UPGRADE_ATTEMPT: Attempting to automatically upgrade the
 FPD image(s) for VSA card in slot 0. Use 'show upgrade fpd progress' command to view the
upgrade progress ...
*Apr 10 00:37:43.023: %FPD_MGMT-6-BUNDLE_DOWNLOAD: Downloading FPD image bundle for VSA
card in slot 0 ...
*Apr 10 00:37:44.543: %FPD_MGMT-6-UPGRADE_TIME: Estimated total FPD image upgrade time for
 VSA card in slot 0 = 00:03:00.
*Apr 10 00:37:44.639: %FPD_MGMT-6-UPGRADE_START: VSA (FPD ID=1) image upgrade in progress
for VSA card in slot 0. Updating to version 0.10. PLEASE DO NOT INTERRUPT DURING THE UPGRADE
 PROCESS (estimated upgrade completion time = 00:03:00) ...****************
*Apr 10 00:38:57.483: %FPD_MGMT-6-UPGRADE_PASSED: VSA (FPD ID=1) image in the VSA card in
slot 0 has been successfully updated from version 0.9 to version 0.10. Upgrading time =
00:01:12.844
*Apr 10 00:38:57.483: %FPD_MGMT-6-OVERALL_UPGRADE: All the attempts to upgrade the required
 FPD images have been completed for VSA card in slot 0. Number of successful/failure
upgrade(s): 1/0.
*Apr 10 00:38:57.483: %FPD_MGMT-5-CARD_POWER_CYCLE: VSA card in slot 0 is being power cycled
 for the FPD image upgrade to take effect.
```

Cisco 7304

The following example shows the output displayed when a SPA requires an FPD image upgrade and the **upgradefpdauto** command is *enabled* . The incompatible FPD image is automatically upgraded.

```
% Uncompressing the bundle ...  [OK]
*Jan 13 22:38:47:%FPD_MGMT-3-INCOMP_FPD_VER:Incompatible 4FE/2GE FPGA (FPD ID=1) image
version detected for SPA-4FE-7304 card in subslot 2/0. Detected version = 4.12, minimal
required version = 4.13. Current HW version = 0.32.
*Jan 13 22:38:47:%FPD_MGMT-5-FPD_UPGRADE_ATTEMPT:Attempting to automatically upgrade the
FPD image(s) for SPA-4FE-7304 card in subslot 2/0 ...

*Jan 13 22:38:47:%FPD_MGMT-6-BUNDLE_DOWNLOAD:Downloading FPD image bundle for SPA-4FE-7304
 card in subslot 2/0 ...
*Jan 13 22:38:49:%FPD_MGMT-6-FPD_UPGRADE_TIME:Estimated total FPD image upgrade time for
SPA-4FE-7304 card in subslot 2/0 = 00:06:00.
```

```
*Jan 13 22:38:49:%FPD_MGMT-6-FPD_UPGRADE_START:4FE/2GE FPGA (FPD ID=1) image upgrade in
progress for SPA-4FE-7304 card in subslot 2/0. Updating to version 4.13. PLEASE DO NOT
INTERRUPT DURING THE UPGRADE PROCESS (estimated upgrade completion time = 00:06:00)
...[...................................................................
(part of the output has been removed for brevity)
.......................................................................................................]
SUCCESS - Completed XSVF execution.

*Jan 13 22:44:33:%FPD_MGMT-6-FPD_UPGRADE_PASSED:4FE/2GE FPGA (FPD ID=1) image upgrade for
SPA-4FE-7304 card in subslot 2/0 has PASSED. Upgrading time = 00:05:44.108
*Jan 13 22:44:33:%FPD_MGMT-6-OVERALL_FPD_UPGRADE:All the attempts to upgrade the required
FPD images have been completed for SPA-4FE-7304 card in subslot 2/0. Number of
successful/failure upgrade(s):1/0.
*Jan 13 22:44:33:%FPD_MGMT-5-CARD_POWER_CYCLE:SPA-4FE-7304 card in subslot 2/0 is being
power cycled for the FPD image upgrade to take effect.
```

Related Commands

Command	Description
show hw-module all fpd	Displays the current versions of all FPDs for all of the supported card types on a router.
show hw-module slot fpd	Displays the current versions of all FPDs for a SIP in the specified slot location and for all of the SPAs installed in that SIP or any FPD-capable cards.
show hw-module subslot fpd	Displays the current versions of all FPDs for a particular SPA or all of the active SPAs on a router.
show upgrade fpd file	Displays the contents of an FPD image package file.
show upgrade fpd package default	Displays which FPD image package is needed for the router to properly support the SPAs or other FPD-capable cards.
show upgrade fpd progress	Displays the progress of the FPD upgrade while an FPD upgrade is taking place.
show upgrade fpd table	Displays various information used by the Cisco IOS software to manage the FPD image package file.
upgrade fpd path	Specifies the location from where the FPD image package should be loaded when an automatic FPD upgrade is initiated by the router.
upgrade hw-module slot	Manually upgrades the current FPD image package on a SIP or any FPD-capable cards.
upgrade hw-module subslot	Manually upgrades the current FPD image on the specified SPA.

upgrade fpd path

To configure the router to search for an FPD image package file in a location other than the default router Flash file system during an automatic FPD upgrade, enter the **upgradefpdpath** command in global configuration mode. To return to the default setting of the router searching for the FPD image package file in the router Flash file systems when an automatic FPD upgrade is triggered, use the **no** form of this command.

upgrade fpd path *fpd-pkg-dir-url*
no upgrade fpd path *fpd-pkg-dir-url*

Syntax Description

fpd-pkg-dir-url	Specifies the location of the FPD image package file, beginning with the location or type of storage device (examples include disk0, slot0, tftp, or ftp) and followed by the path to the FPD image package file. It is important to note that the name of the FPD image package file should not be specified as part of *fpd-pkg-dir-url*; Cisco IOS will automatically download the correct FPD image package file once directed to the proper location. It is important to note that the last character of the *fpd-pkg-dir-url* is always a "/".

Command Default

The **upgradefpdpath** command is used to specify a new location for a router to locate the FPD image package file, if you want to store the FPD image package file in a location other than the default router Flash file system for automatic FPD upgrades. The default locations the router searches are as follows:

The router searches the disk2: Flash Disk for the FPD image package file when an FPD incompatibility is detected and **upgradefpdauto** is enabled.

The **routersearchesthe**primary Flash file system (disk0:) for the FPD image package file when an FPD incompatibility is detected and **upgradefpdauto** is enabled.

The router searches all of its Flash file systems for the FPD image package when an FPD incompatibility is detected and **upgradefpdauto** is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(20)S2	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(4)XD3	This command was integrated into Cisco IOS Release 12.4(4)XD3.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

It is important to note that the last character of the *fpd-pkg-dir-url* is always a "/". This path points users to the directory that stores the file, but not the file itself.

When specifying the path to the location of the new FPD image package file, do not include the file name in the path. The Cisco IOS will automatically download the correct FPD image package file once directed to the proper location, even if multiple FPD image package files of different versions are stored in the same location.

If the **upgradefpdpath** command is not entered, the router searches the default router Flash file system for the FPD image.

For more information about FPD upgrades on SPA interface processors (SIPs) and shared port adapters (SPAs), refer to the Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide.

Examples

In the following example, the FPD image package file that is stored on the TFTP server using the path johnstftpserver/fpdfiles is scanned for the latest FPD image package file when an automatic FPD upgrade occurs:

```
upgrade fpd path tftp://johnstftpserver/fpdfiles/
```

In the following example, the FPD package file that is stored on the FTP server using the path johnsftpserver/fpdfiles is scanned for the latest FPD image package when an automatic FPD upgrade occurs. In this example, john is the username and XXXXXXX is the FTP password:

```
upgrade fpd path ftp://john:XXXXXXX@johnsftpserver/fpdfiles/
```

Related Commands

Command	Description
show hw-module all fpd	Displays the current versions of all FPDs for all of the supported card types on a router.
show hw-module slot fpd	Displays the current versions of all FPDs for a SIP in the specified slot location and for all of the SPAs installed in that SIP or any FPD-capable cards.
show hw-module subslot fpd	Displays the current versions of all FPDs for a particular SPA or all of the active SPAs on a router.
show upgrade fpd file	Displays the contents of an FPD image package file.
show upgrade fpd package default	Displays which FPD image package is needed for the router to properly support the SPAs or other FPD-capable cards.
show upgrade fpd progress	Displays the progress of the FPD upgrade while an FPD upgrade is taking place.
show upgrade fpd table	Displays various information used by the Cisco IOS software to manage the FPD image package file.
upgrade fpd auto	Configures the router to automatically upgrade the FPD image when an FPD version incompatibility is detected.
upgrade hw-module slot	Manually upgrades the current FPD image package on a SIP or any FPD-capable cards.
upgrade hw-module subslot	Manually upgrades the current FPD image on the specified SPA.

upgrade fpga

To set router behavior regarding handling of FPGA mismatches after FPGA mismatches are detected, use the **upgradefpga** command in privileged EXEC mode.

upgrade fpga [{**force** | **prompt**}]
no upgrade fpga

Syntax Description

force	If the **force** option is entered, an FPGA upgrade will be forced on the system if an FPGA mismatch is detected.
prompt	If the **prompt** option is entered, the user will be prompted to upgrade the FPGA when an FPGA mismatch is detected.

Command Default

Before Cisco IOS Release 12.2(20)S6, users were automatically prompted for an FPGA upgrade when an FPGA version mismatch was detected.

In Cisco IOS Release 12.2(20)S6, the default setting became **noupgradefpga**. By default, FPGA is not upgraded when an FPGA version mismatch is detected and the user is not prompted to upgrade the FPGA, although it is important to note that a message indicating the FPGA mismatch is displayed on the console. Users who want to upgrade FPGA must use the **upgradefpgaall** command to manually perform the upgrade when the default settings are set.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(20)S4	The **upgradefpgaprompt**command was introduced
12.2(20)S6	The **noupgradefpga** command was introduced and became the default setting. The **force** option was introduced. The **noupgradefpgaprompt** command behavior was changed. The **noupgradefpgaprompt** configuration no longer automatically begins an FPGA upgrade when an FPGA mismatch is detected.

Usage Guidelines

Note that **noupgradefpga** is the default setting starting in Cisco IOS Release 12.2(20)S6. See the Defaults section of this command reference for additional information on the changes to the default setting in Cisco IOS Release 12.2(20)S6.

This command can be used to upgrade all of the FPGAs in a Cisco 7304 router except for the SPA FPGA. The SPA FPGA is upgraded using an FPD image package.

An FPGA match check is automatically run by the Cisco 7304 router during system bootup or after a piece of hardware with FPGA is installed into an operating Cisco 7304 router. This command defines the behavior for a router after an FPGA mismatch is detected during one of these FPGA match checks. When the default setting of **noupgradefpga** is maintained, FPGA is not upgraded when an FPGA mismatch is detected and the user is not prompted regarding an FPGA upgrade. If the **upgradefpgaprompt** command is entered, a prompt asking users whether they would like to perform an FPGA upgrade appears on the console when FPGA mismatches are detected. If the **upgradefpgaforce** command is entered, an FPGA upgrade occurs automatically when an FPGA mismatch is detected.

In Cisco IOS Releases 12.2(20)S4 and 12.2(20)S5, the **noupgradefpgaprompt** configuration automatically started an FPGA upgrade when an FPGA mismatch was detected. Starting in Cisco IOS Release 12.2(20)S6, the **noupgradefpgaprompt** configuration is the same configuration as **noupgradefpga**. When this setting of **noupgradefpga** is maintained, the FPGA is not upgraded when an FPGA mismatch is detected and the user is not prompted regarding an FPGA upgrade.

While the **noupgradefpga** command can be entered as a configuration command, the **upgradefpga** command cannot be entered unless the **force** or **prompt** options are also entered.

The **force** or **prompt** options are not necessary when entering the no upgrade fpga command. The options can be entered, but the system configuration will revert to the **noupgradefpga** configuration regardless of whether a keyword is entered.

Note that when the FPGA prompt is configured, the prompt appears on the console screen only. If you are connecting to a router using a telnet connection through a line card, SPA, or port adapter, you will not see this prompt. If you are connecting to the router through one of these methods, we recommend not configuring **upgradefpgaprompt** because you will not be able to see the prompt and the prompt will time out.

Examples

In the following example, the system configuration has been changed so that users will be prompted regarding an FPGA upgrade if an FPGA mismatch is detected during bootup or after an OIR hardware insertion.

```
Router# upgrade fpga prompt
```

The following example is the output of a router that has detected an FPGA mismatch when the **upgradefpgaprompt**command is configured. Note the “Upgrade slot 5 LC FPGA? [y/n]” prompt. In this example, the prompt is answered and the FPGA upgrade is performed.

```
The following board(s) have an FPGA image that is different
from the IOS bundled FPGA image
Please note the board(s) will be reset after FPGA update.
In the case of NSE, it will reload the whole system.
                          HARDWARE        FPGA VERSION ESTIMATED TIME
SLOT  FPGA                VERSION    CURRENT    IOS BUNDLED    TO UPDATE
----  ----                --------   -------    ----------- --------------
 5    6T3                  03.03      00.20        00.21       up to 12 minutes
Upgrade slot 5 LC FPGA? [y/n]y
Slot 5 LC FPGA update in process
PLEASE DO NOT INTERRUPT DURING FPGA UPDATE PROCESS
OR NEXT RELOAD MAY CRASH THE SYSTEM
FPGA flash update in progress
Erasing (this may take a while)...
Programming...
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
Verifying FPGA flash
  Reading from FPGA
flash...vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvDone

  Comparing with the source file...Passed
Slot 5 LC FPGA successfully updated from version 00.20 to version 00.21
Slot 5 linecard reset after FPGA update...
Slot 5 linecard successfully reset
```

In the following example, the system configuration has been changed so that an FPGA upgrade will occur automatically if an FPGA mismatch is detected during bootup or after an OIR hardware insertion:

```
Router# upgrade fpga force
```

The following example is from a router that has detected an FPGA mismatch when **upgradefpgaforce** is configured. Note that the upgrade occurs automatically without the user being prompted for any information.

```
The following board(s) have an FPGA image that is different
from the IOS bundled FPGA image
Please note the board(s) will be reset after FPGA update.
In the case of NSE, it will reload the whole system.
                          HARDWARE        FPGA VERSION ESTIMATED TIME
SLOT  FPGA                VERSION    CURRENT    IOS BUNDLED    TO UPDATE
----  ----                --------   -------    ----------- --------------
 5    6T3                  03.03      00.20        00.21       up to 12 minutes
Slot 5 LC FPGA update in process
PLEASE DO NOT INTERRUPT DURING FPGA UPDATE PROCESS
OR NEXT RELOAD MAY CRASH THE SYSTEM
FPGA flash update in progress
Erasing (this may take a while)...
Programming...
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Verifying FPGA flash
  Reading from FPGA
flash...vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvDone

  Comparing with the source file...Passed
Slot 5 LC FPGA successfully updated from version 00.20 to version 00.21
Slot 5 linecard reset after FPGA update...
Slot 5 linecard successfully reset
```

In the following example, the default configuration where no prompt and no forced upgrade occurs when an FPGA mismatch occurs is restored.

```
Router# no upgrade fpga
```

The following example is from a router that has detected an FPGA mismatch when **noupgradefpga** is configured. Note that the FPGA upgrade was not performed. If you receive these messages and want to upgrade FPGA, enter the **upgradefpgaall** command to manually perform an FPGA upgrade.

```
00:00:05:%PLATFORM-4-FPGA_MISMATCH:FPGA image in slot 0 (name = NPEG100, hardware version
= 01.00, current fpga version = 02.04) does not match the FPGA image in Cisco IOS software
 (version 02.05). Approximate time to update the FPGA image is 12 minutes.
00:00:08:%PLATFORM-4-FPGA_MISMATCH:FPGA image in slot 5 (name = 6T3, hardware version =
03.03, current fpga version = 00.20) does not match the FPGA image in Cisco IOS software
(version 00.21). Approximate time to update the FPGA image is 12 minutes.
```

Related Commands

Command	Description
show c7300	Displays the types of hardware installed in a Cisco 7304 router, including the current FPGA version and the bundled FPGA version.
show diag	Displays hardware information for any slot or the chassis.

Command	Description
show upgrade fpga progress	Displays the progress of an FPGA upgrade.
upgrade fpga all	Manually upgrades all of the FPGAs for all of the installed hardware on the Cisco 7304 router.

upgrade fpga all

To manually start the Field-Programmable Gate Array (FPGA) image update process, use the **upgradefpgaall**command in privileged EXEC mode.

upgrade fpga all

Syntax Description

This command has no arguments or keywords.

Command Default

No default behaviors or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EX	This command was introduced.
12.2(11)YZ	Support was added for the 7300-CC-PA.
12.2(18)S	This command was introduced on Cisco 7304 routers running Cisco IOS Release 12.2 S.
12.2(20)S6	The prompt asking users if they would like to reload the line card to complete the FPGA upgrade process was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to manually start the FPGA image update process. Automatic FPGA version checking is performed during every system startup for all line cards, processors, and jacket cards in the system. Automatic FPGA version checking is also performed for hardware after insertion of that hardware during an online insertion and removal (OIR).

Traffic disruption for traffic on the hardware upgrading FPGA usually occurs during FPGA upgrades. If you are going to upgrade FPGA using this command, keep this fact in mind.

Before Cisco IOS Release 12.2(20)S6, the hardware that had the FPGA upgrade would automatically be reloaded as the final procedure of the FPGA upgrade. In Cisco IOS Release 12.2(20)S6 onward, the user sees a prompt asking if the hardware should be reloaded to complete the FPGA upgrade. The user can choose to skip the hardware reload at the current time if desired, but the FPGA upgrade is not complete until the hardware is reloaded. If the user chooses not to reload the hardware that is getting the FPGA upgrade, the hardware will have to be reloaded using the **hw-module***slot-number***stop** command followed by the **hw-module***slot-number***start** command if the hardware is not a processor. If the hardware is a processor, the router must be reloaded.

In cases where the FPGA upgrade is performed but the hardware is not reloaded, users should note that the bundled FPGA version will be transferred to Flash memory but not to the hardware. Therefore, if the **showc7300** command is entered to see FPGA versions after an FPGA upgrade has been performed but not completed by reloading the hardware, the bundled FPGA version should match the Flash memory version. After the hardware is reloaded, the bundled, the Flash, and the system FPGA should all match and the upgrade should be complete.

Examples

The following example shows a manual FPGA upgrade for a router using Cisco IOS Release 12.2(20)S6 or later. Note that the user elects to reject the NPE-G100 upgrade. More importantly, note the user is prompted about reloading the 6T3 line card to complete the FPGA upgrade after electing to perform that FPGA upgrade. In this example, the user decides to reject the card reload for the 6T3 line card in slot 5 and the FPGA upgrade for that card is not finalized.

```
Router# upgrade fpga all
The following board(s) have an FPGA image that is different
from the IOS bundled FPGA image
                          HARDWARE        FPGA VERSION ESTIMATED TIME
SLOT  FPGA                VERSION    CURRENT    IOS BUNDLED    TO UPDATE
----  ----                --------   -------    ----------- --------------
 0    NPEG100              01.00      02.04        02.05       up to 12 minutes
 5    6T3                  03.03      00.20        00.21       up to 12 minutes
Upgrade slot 0 NPEG100 FPGA? [y/n]n
%Warning:FPGA update skipped
Slot 0 NPEG100 FPGA may contain incompatible FPGA version.
This may cause system to be unstable.
00:07:54:%PLATFORM-6-FPGAUPDSKIP:Slot 0 NPEG100 FPGA update skipped.
Upgrade slot 5 LC FPGA? [y/n]y
The card in slot 5 should be reloaded for the new FPGA image to take effect.
Do you want to reload the card? [Y/N]n
Slot 5 LC FPGA update in process
PLEASE DO NOT INTERRUPT DURING FPGA UPDATE PROCESS
OR NEXT RELOAD MAY CRASH THE SYSTEM
FPGA flash update in progress
Erasing (this may take a while)...
Programming...
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Verifying FPGA flash
  Reading from FPGA
flash...vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvDone

  Comparing with the source file...Passed
Slot 5 LC FPGA successfully updated from version 00.20 to version 00.21
00:20:27:%PLATFORM-6-FPGAUPDSUCCESS:Slot 5 LC FPGA successfully updated from version 00.20
 to 00.21.
00:20:27:%PLATFORM-4-FPGAUPD_RELOAD_SKIP:After the FPGA update, the card in slot 5 was not
 reloaded. The card should be reloaded for the new FPGA image to take effect.
```

The following example shows how to manually start the FPGA image update process for an NSE for a router running a pre-Cisco IOS Release 12.2(20)S6 software image:

```
Router# upgrade fpga all
The following board(s) may have incompatible FPGA(s) and may
need an upgrade or downgrade.
Please note the board(s) will be reset after FPGA update.
In the case of NSE, it will reload the whole system.
SLOT  FPGA                CURRENT VERSION  BUNDLED VERSION  ESTIMATED TIME TO
                           ON THE BOARD         IN IOS            UPDATE
----  ----                ---------------  ---------------  -----------------
 0    NSE100 (MB)              00.03            00.12       up to 15 minutes
 0    NSE100 (DB)              00.03            00.10       up to 6 minutes
Upgrade slot 0 NSE MB FPGA? [y/n]y
Upgrade slot 0 NSE DB FPGA? [y/n]y
Slot 0 NSE MB FPGA update in process
PLEASE DO NOT INTERRUPT DURING FPGA UPDATE PROCESS
OR NEXT RELOAD MAY CRASH THE SYSTEM
FPGA flash update in progress
Erasing (this may take a while)...
Programming...
```

```
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Verifying FPGA flash
  Reading from FPGA flash...vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv
 vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv
 vvvvvvvvvvvvvDone
Comparing with the source file...Passed
Slot 0 NSE MB FPGA successfully updated from version 0.3 to version 0.12
Slot 0 NSE DB FPGA update in process
PLEASE DO NOT INTERRUPT DURING FPGA UPDATE PROCESS
OR NEXT RELOAD MAY CRASH THE SYSTEM
FPGA flash update in progress
Erasing (this may take a while)...
Programming...
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Verifying FPGA flash
  Reading from FPGA flash...vvvvvvvvvvvvvvvvvvvvvDone
  Comparing with the source file...Passed
Slot 0 NSE DB FPGA successfully updated from version 0.3 to version 0.10
System will be reloaded now for the new FPGA to take effect...
```

The following example shows how to manually update the FPGA image of a line card on a router running pre-Cisco IOS Release 12.2(20)S6 software:

```
Router# upgrade fpga all
The following board(s) may have incompatible FPGA(s) and may
need an upgrade or downgrade.
Please note the board(s) will be reset after FPGA update.
In the case of NSE, it will reload the whole system.
SLOT  FPGA                CURRENT VERSION  BUNDLED VERSION  ESTIMATED TIME TO
                           ON THE BOARD         IN IOS             UPDATE
----  ----                ---------------  ---------------  -----------------
 4    OC48 POS                 00.13            00.12       up to 5 minutes
Downgrade slot 4 LC FPGA? [y/n]y
Slot 4 LC FPGA update in process
PLEASE DO NOT INTERRUPT DURING FPGA UPDATE PROCESS
OR NEXT RELOAD MAY CRASH THE SYSTEM
FPGA flash update in progress
Erasing (this may take a while)...
Programming...
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Verifying FPGA flash
  Reading from FPGA flash...vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvDone
  Comparing with the source file...Passed
Slot 4 LC FPGA successfully updated from version 0.13 to version 0.12
Slot 4 linecard reset after FPGA update...
Slot 4 linecard successfully reset
00:11:37:%PLATFORM-6-FPGAUPDSUCCESS:Slot 4 LC FPGA successfully update from version 0.13
to 0.12.
```

Related Commands

Command	Description
show c7300	Displays the types of hardware (processors, line cards, jacket cards, and so on) installed in the Cisco 7304 router slots, including the bundled, Flash, and current FPGA versions.
show diag	Displays hardware information for any slot or the chassis.
upgrade rom-monitor default	Configures a particular ROM monitor image as the default ROMmon image.

Command	Description
upgrade rom-monitor file	Upgrades the ROM monitor.

upgrade hw-module slot

Note The upgrade hw-module slot command is not available in Cisco IOS Release 12.2(33)SRB and later Cisco IOS 12.2SR releases. It is replaced by the upgrade hw-module slot fpd file command.

Note The upgrade hw-module slot command is not available in Cisco IOS Release 12.4(15)T and later Cisco IOS 12.4T releases. It is replaced by the upgrade hw-module slot fpd file command.

To manually upgrade the current FPD image package on a SIP or any FPD-capable cards, enter the **upgradehw-moduleslot** command in privileged EXEC mode.

Cisco 7200 VXR
upgrade hw-module slot {*slot* | **npe**} **file** *file-url*

Cisco 7600 Series
upgrade hw-module slot *slot* **file** *file-url* [**force**]

Syntax Description

slot	Chassis slot number. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide. For slot numbering in the Cisco 7200 VXR router, refer to refer to the Cisco 7200 VXR Installation and Configuration Guide.
npe	NPE-G2 network processing engine in the Cisco 7200 VXR router.
file	Specifies that a file will be downloaded.
file-url	Specifies the location of the FPD image package file, beginning with the location or type of storage device (examples include **disk0**, **slot0**, **tftp**, or **ftp**) and followed by the path to the FPD image package file.
force	(Optional) Forces the update of all compatible FPD images in the indicated FPD image package file on the SPA that meet the minimal version requirements. Without this option, the manual upgrade will only upgrade incompatible FPD images.

Command Default

No default behavior or values.

No default behavior or values, although it is important to note that the router containing the SIP is configured, by default, to upgrade the FPD images when it detects a version incompatibility between the FPD image on the SIP and the FPD image required to run the SPA with the running Cisco IOS image. The **upgradehw-moduleslot** command is used to manually upgrade the FPD images; therefore, the **upgradehw-moduleslot**command should only be used when the automatic upgrade default configuration fails to find a compatible FPD image for one of the SPAs or when the automatic upgrade default configuration has been manually disabled. The **noupgradefpdauto** command can be entered to disable automatic FPD upgrades.

If no FPD incompatibility is detected, this command will not upgrade SPA FPD images unless the **force** option is entered.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(4)XD	This command was integrated into Cisco IOS Release 12.4(4)XD, and the npe keyword was added.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was removed. It is not available in Cisco IOS Release 12.2(33)SRB and later Cisco IOS 12.2SR releases. It is replaced by the upgrade hw-module slot fpd file command.
12.4(15)T	This command was removed. It is not available in Cisco IOS Release 12.4(15)T and later Cisco IOS 12.4T releases. It is replaced by the upgrade hw-module slot fpd file command.

Usage Guidelines

Cisco 7200 VXR

This command is used to manually upgrade FPD images. Note that for a manual FPD upgrade to take effect on the NPE-G2, you must power cycle the router. The router will not use the new version of the NPE-G2 FPD image if you reload the router without a power cycle. Other FPD-capable cards require only a router reload after a manual FPD upgrade, not a router power cycle.

Cisco 7600 Series

This command is used to manually upgrade the FPD images on a SIP. In most cases, the easiest and recommended method of upgrading FPD images is the automatic FPD upgrade, which is enabled by default. The automatic FPD upgrade detects and automatically upgrades all FPD images when an FPD incompatibility is detected.

A manual FPD upgrade is usually used in the following situations:

- The target SIP was disabled by the system because of an incompatible FPD image (the system could not find the required FPD image package file).
- A recovery upgrade must be performed.
- A special bug fix to an FPD image is provided in the FPD image package file.

The FPD image upgrade process places the SIP and all the SPAs in the SIP offline. The time required to complete an FPD image upgrade can be lengthy. The **showupgradefpdprogress** command can be used to gather more information about estimated FPD image download times for a particular SIP.

For more information about FPD upgrades on SPA interface processors (SIPs) and shared port adapters (SPAs), see the Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide. For FPD upgrades on the Cisco 7200 VXR router, see the *Field-Programmable Device Upgrades* feature guide.

Examples

Cisco 7200 VXR

The following example shows a sample manual FPD upgrade of the FPD image package for the NPE-G2:

```
Router# upgrade hw-module slot npe file
tftp://mytftpserver/myname/myfpdpkg/c7200-fpd-pkg.124-4.XD.pkg
% The following FPD(s) will be updated for NPE-G2 (H/W ver = 0.0) in NPE slot:
         ================== =========== =========== ============
         Field Programmable   Current     Upgrade   Estimated
         Device: "ID-Name"    Version     Version   Upgrade Time
         ================== =========== =========== ============
         1-NPEG2 I/O FPGA       0.7         0.8       00:01:00
         ================== =========== =========== ============
% NOTES:
  - Use 'show upgrade fpd progress' command to view the progress of the FPD
    upgrade.
  - The target card will be automatically reload after the upgrade
    operation. This reload will interrupt normal operation of the card. If
    necessary, ensure that appropriate actions have been taken to redirect
    card traffic before starting the FPD upgrade.
% Are you sure that you want to perform this operation? [no]: yes
% Initiating the upgrade operation on the target card ...
Router#
*Jan  1 00:33:41.611: %FPD_MGMT-6-UPGRADE_TIME: Estimated total FPD image upgrade time for
 NPE-G2 card in NPE slot = 00:01:00.
*Jan  1 00:33:41.615: %FPD_MGMT-6-UPGRADE_START: NPEG2 I/O FPGA (FPD ID=1) image upgrade
in progress for NPE-G2 card in NPE slot. Updating to version 0.8. PLEASE DO NOT INTERRUPT
DURING THE UPGRADE PROCESS (estimated upgrade completion time = 00:01:00) ...
*Jan  1 00:34:14.279: %FPD_MGMT-6-UPGRADE_PASSED: NPEG2 I/O FPGA (FPD ID=1) image in the
NPE-G2 card in NPE slot has been successfully updated from version 0.7 to version 0.8.
Upgrading time = 00:00:32.664
*Jan  1 00:34:14.279: %FPD_MGMT-6-OVERALL_UPGRADE: All the attempts to upgrade the required
 FPD images have been completed for NPE-G2 card in NPE slot. Number of successful/failure
upgrade(s): 1/0.
*Jan  1 00:34:14.279: %FPD_MGMT-5-CARD_POWER_CYCLE: NPE-G2 card in NPE slot is being power
 cycled for the FPD image upgrade to take effect.
```

Cisco 7600 Series

The following example shows a sample manual FPD upgrade:

```
Router# upgrade hw-module slot 4 file disk0:c7600-fpd-pkg.122-18.SXE.pkg

% The following FPD(s) will be upgraded for 7600-SIP-200 (H/W ver = 0.550) in slot 4:
    ================== =========== =========== ============
    Field Programmable   Current     Upgrade   Estimated
    Device:"ID-Name"   Version     Version   Upgrade Time
    ================== =========== =========== ============
    5-ROMMON              1.1         1.2       00:02:00
    ================== =========== =========== ============
% Are you sure that you want to perform this operation? [no]:y

% Restarting the target card in slot 4 for FPD image upgrade. Please wait ...
Router#
Mar 25 16:39:37:%CWAN_RP-6-CARDRELOAD:Module reloaded on slot 4/0
SLOT 4:00:00:06:%SSA-5-FABRICSYNC_DONE:Fabric sync on Primary channel done.
Mar 25 16:39:40:%MLS_RATE-4-DISABLING:The Layer2 Rate Limiters have been disabled.
```

```
Mar 25 16:39:40:%FPD_MGMT-6-UPGRADE_TIME:Estimated total FPD image upgrade time for
7600-SIP-200 card in slot 4 = 00:02:00.
Mar 25 16:39:40:%FPD_MGMT-6-UPGRADE_START:ROMMON (FPD ID=5) image upgrade in progress for
7600-SIP-200 card in slot 4. Updating to version 1.2. PLEASE DO NOT INTERRUPT DURING THE
UPGRADE PROCESS (estimated upgrade completion time = 00:02:00) ...
Mar 25 16:39:39:%DIAG-SP-6-RUN_COMPLETE:Module 4:Running Complete Diagnostics...
Mar 25 16:39:40:%DIAG-SP-6-DIAG_OK:Module 4:Passed Online Diagnostics
SLOT 1:Mar 26 00:39:40:%SSA-5-FABRICSYNC_DONE:Fabric sync on Primary channel done.
Mar 25 16:39:40:%OIR-SP-6-INSCARD:Card inserted in slot 4, interfaces are now online
Mar 25 16:39:46:%FPD_MGMT-6-UPGRADE_PASSED:ROMMON (FPD ID=5) image in the 7600-SIP-200 card
 in slot 4 has been successfully updated from version 1.1 to version 1.2. Upgrading time =
 00:00:06.000
Mar 25 16:39:46:%FPD_MGMT-6-OVERALL_UPGRADE:All the attempts to upgrade the required FPD
images have been completed for 7600-SIP-200 card in slot 4. Number of successful/failure
upgrade(s):1/0.
Mar 25 16:39:47:%FPD_MGMT-5-CARD_POWER_CYCLE:7600-SIP-200 card in slot 4 is being power
cycled for the FPD image upgrade to take effect.
Mar 25 16:39:47:%OIR-6-REMCARD:Card removed from slot 4, interfaces disabled
Mar 25 16:39:47:%C6KPWR-SP-4-DISABLED:power to module in slot 4 set off (Reset)
Mar 25 16:40:38:%CWAN_RP-6-CARDRELOAD:Module reloaded on slot 4/0
SLOT 4:00:00:06:%SSA-5-FABRICSYNC_DONE:Fabric sync on Primary channel done.
Mar 25 16:40:41:%MLS_RATE-4-DISABLING:The Layer2 Rate Limiters have been disabled.
Mar 25 16:40:40:%DIAG-SP-6-RUN_COMPLETE:Module 4:Running Complete Diagnostics...
Mar 25 16:40:41:%DIAG-SP-6-DIAG_OK:Module 4:Passed Online Diagnostics
SLOT 1:Mar 26 00:40:41:%SSA-5-FABRICSYNC_DONE:Fabric sync on Primary channel done.
Mar 25 16:40:41:%OIR-SP-6-INSCARD:Card inserted in slot 4, interfaces are now online
```

Related Commands

Command	Description
show hw-module all fpd	Displays the current versions of all FPDs for all of the supported card types on a router.
show hw-module slot fpd	Displays the current versions of all FPDs for a SIP in the specified slot location and for all of the SPAs installed in that SIP or any FPD-capable cards.
show hw-module subslot fpd	Displays the current versions of all FPDs for a particular SPA or all of the active SPAs on a router.
show upgrade fpd file	Displays the contents of an FPD image package file.
show upgrade fpd package default	Displays which FPD image package is needed for the router to properly support the SPAs or other FPD-capable cards.
show upgrade fpd progress	Displays the progress of the FPD upgrade while an FPD upgrade is taking place.
show upgrade fpd table	Displays various information used by the Cisco IOS software to manage the FPD image package file.
upgrade fpd auto	Configures the router to automatically upgrade the FPD image when an FPD version incompatibility is detected.
upgrade fpd path	Specifies the location from where the FPD image package should be loaded when an automatic FPD upgrade is initiated by the router.
upgrade hw-module subslot	Manually upgrades the current FPD image on the specified SPA.

upgrade hw-module slot fpd file

To manually upgrade the current FPD image package on a SIP or any FPD-capable cards, use the **upgradehw-moduleslotfpdfile**command in privileged EXEC mode.

Cisco 7200 VXR
upgrade hw-module slot {*slot* | **npe**} *fpd* **file** *file-url*

Cisco 7600 Series
upgrade hw-module slot *slot* **fpd file** *file-url* [**force**]

Syntax Description

slot	Chassis slot number. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide. For slot numbering in the Cisco 7200 VXR router, refer to refer to the Cisco 7200 VXR Installation and Configuration Guide .
npe	NPE-G2 network processing engine in the Cisco 7200 VXR router.
file-url	Specifies the location of the FPD image package file, beginning with the location or type of storage device (examples include **disk0**, **slot0**, **tftp**, or **ftp**) and followed by the path to the FPD image package file.
force	(Optional) Forces the update of all compatible FPD images in the indicated FPD image package file on the SPA that meet the minimal version requirements. Without this option, the manual upgrade will only upgrade incompatible FPD images.

Command Default

No default behavior or values.

No default behavior or values, although it is important to note that the router containing the SIP is configured, by default, to upgrade the FPD images when it detects a version incompatibility between the FPD image on the SIP and the FPD image required to run the SPA with the running Cisco IOS image. Manual upgrade of FPD images is recommended only when the automatic upgrade default configuration fails to find a compatible FPD image for one of the SPAs, or when the automatic upgrade default configuration has been manually disabled. The **noupgradefpdauto** command can be entered to disable automatic FPD upgrades.

If no FPD incompatibility is detected, this command will not upgrade SPA FPD images unless the **force** option is entered.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRB	This command was introduced. This command replaces the upgrade hw-module slot command.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

Cisco 7200 VXR

This command is used to manually upgrade FPD images. In most cases, the easiest and recommended method of upgrading FPD images is the automatic FPD upgrade, which is enabled by default. Note that for a manual FPD upgrade to take effect on the NPE-G2, you must power cycle the router. The router will not use the new version of the NPE-G2 FPD image if you reload the router without a power cycle. Other FPD-capable cards require only a router reload after a manual FPD upgrade, not a router power cycle.

Cisco 7600 Series

This command is used to manually upgrade the FPD images on a SIP. In most cases, the easiest and recommended method of upgrading FPD images is the automatic FPD upgrade, which is enabled by default. The automatic FPD upgrade detects and automatically upgrades all FPD images when an FPD incompatibility is detected.

A manual FPD upgrade is usually used in the following situations:

- The target SIP was disabled by the system because of an incompatible FPD image (the system could not find the required FPD image package file).
- A recovery upgrade must be performed.
- A special bug fix to an FPD image is provided in the FPD image package file.

The FPD image upgrade process places the SIP and all the SPAs in the SIP offline. The time required to complete an FPD image upgrade can be lengthy. The **showupgradefpdprogress** command can be used to gather more information about estimated FPD image download times for a particular SIP.

For more information about FPD upgrades on SPA interface processors (SIPs) and shared port adapters (SPAs), see the Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide. For FPD upgrades on the Cisco 7200 VXR router, see the *Field-Programmable Device Upgrades* feature guide.

Examples

Cisco 7200 VXR

The following example shows a sample manual FPD upgrade of the FPD image package for the NPE-G2:

```
Router# upgrade hw-module slot npe fpd file
tftp://mytftpserver/myname/myfpdpkg/c7200-fpd-pkg.124-4.XD.pkg
% The following FPD(s) will be updated for NPE-G2 (H/W ver = 0.0) in NPE slot:
         ================== =========== =========== ============
         Field Programmable   Current     Upgrade   Estimated
         Device: "ID-Name"    Version     Version   Upgrade Time
         ================== =========== =========== ============
         1-NPEG2 I/O FPGA       0.7         0.8       00:01:00
         ================== =========== =========== ============
% NOTES:
  - Use 'show upgrade fpd progress' command to view the progress of the FPD
    upgrade.
  - The target card will be automatically reload after the upgrade
    operation. This reload will interrupt normal operation of the card. If
    necessary, ensure that appropriate actions have been taken to redirect
    card traffic before starting the FPD upgrade.
% Are you sure that you want to perform this operation? [no]: yes
% Initiating the upgrade operation on the target card ...
Router#
*Jan  1 00:33:41.611: %FPD_MGMT-6-UPGRADE_TIME: Estimated total FPD image upgrade time for
 NPE-G2 card in NPE slot = 00:01:00.
*Jan  1 00:33:41.615: %FPD_MGMT-6-UPGRADE_START: NPEG2 I/O FPGA (FPD ID=1) image upgrade
```

```
in progress for NPE-G2 card in NPE slot. Updating to version 0.8. PLEASE DO NOT INTERRUPT
DURING THE UPGRADE PROCESS (estimated upgrade completion time = 00:01:00) ...
*Jan  1 00:34:14.279: %FPD_MGMT-6-UPGRADE_PASSED: NPEG2 I/O FPGA (FPD ID=1) image in the
NPE-G2 card in NPE slot has been successfully updated from version 0.7 to version 0.8.
Upgrading time = 00:00:32.664
*Jan  1 00:34:14.279: %FPD_MGMT-6-OVERALL_UPGRADE: All the attempts to upgrade the required
 FPD images have been completed for NPE-G2 card in NPE slot. Number of successful/failure
upgrade(s): 1/0.
*Jan  1 00:34:14.279: %FPD_MGMT-5-CARD_POWER_CYCLE: NPE-G2 card in NPE slot is being power
 cycled for the FPD image upgrade to take effect.
```

Cisco 7600 Series

The following example shows a sample manual FPD upgrade:

```
Router# upgrade hw-module slot 4
fpd file disk0:c7600-fpd-pkg.122-18.SXE.pkg

% The following FPD(s) will be upgraded for 7600-SIP-200 (H/W ver = 0.550) in slot 4:
    ================== =========== =========== ============
    Field Programmable   Current     Upgrade   Estimated
    Device:"ID-Name"    Version     Version   Upgrade Time
    ================== =========== =========== ============
    5-ROMMON               1.1         1.2       00:02:00
    ================== =========== =========== ============
% Are you sure that you want to perform this operation? [no]:y

% Restarting the target card in slot 4 for FPD image upgrade. Please wait ...
Router#
Mar 25 16:39:37:%CWAN_RP-6-CARDRELOAD:Module reloaded on slot 4/0
SLOT 4:00:00:06:%SSA-5-FABRICSYNC_DONE:Fabric sync on Primary channel done.
Mar 25 16:39:40:%MLS_RATE-4-DISABLING:The Layer2 Rate Limiters have been disabled.
Mar 25 16:39:40:%FPD_MGMT-6-UPGRADE_TIME:Estimated total FPD image upgrade time for
7600-SIP-200 card in slot 4 = 00:02:00.
Mar 25 16:39:40:%FPD_MGMT-6-UPGRADE_START:ROMMON (FPD ID=5) image upgrade in progress for
7600-SIP-200 card in slot 4. Updating to version 1.2. PLEASE DO NOT INTERRUPT DURING THE
UPGRADE PROCESS (estimated upgrade completion time = 00:02:00) ...
Mar 25 16:39:39:%DIAG-SP-6-RUN_COMPLETE:Module 4:Running Complete Diagnostics...
Mar 25 16:39:40:%DIAG-SP-6-DIAG_OK:Module 4:Passed Online Diagnostics
SLOT 1:Mar 26 00:39:40:%SSA-5-FABRICSYNC_DONE:Fabric sync on Primary channel done.
Mar 25 16:39:40:%OIR-SP-6-INSCARD:Card inserted in slot 4, interfaces are now online
Mar 25 16:39:46:%FPD_MGMT-6-UPGRADE_PASSED:ROMMON (FPD ID=5) image in the 7600-SIP-200 card
 in slot 4 has been successfully updated from version 1.1 to version 1.2. Upgrading time =
 00:00:06.000
Mar 25 16:39:46:%FPD_MGMT-6-OVERALL_UPGRADE:All the attempts to upgrade the required FPD
images have been completed for 7600-SIP-200 card in slot 4. Number of successful/failure
upgrade(s):1/0.
Mar 25 16:39:47:%FPD_MGMT-5-CARD_POWER_CYCLE:7600-SIP-200 card in slot 4 is being power
cycled for the FPD image upgrade to take effect.
Mar 25 16:39:47:%OIR-6-REMCARD:Card removed from slot 4, interfaces disabled
Mar 25 16:39:47:%C6KPWR-SP-4-DISABLED:power to module in slot 4 set off (Reset)
Mar 25 16:40:38:%CWAN_RP-6-CARDRELOAD:Module reloaded on slot 4/0
SLOT 4:00:00:06:%SSA-5-FABRICSYNC_DONE:Fabric sync on Primary channel done.
Mar 25 16:40:41:%MLS_RATE-4-DISABLING:The Layer2 Rate Limiters have been disabled.
Mar 25 16:40:40:%DIAG-SP-6-RUN_COMPLETE:Module 4:Running Complete Diagnostics...
Mar 25 16:40:41:%DIAG-SP-6-DIAG_OK:Module 4:Passed Online Diagnostics
SLOT 1:Mar 26 00:40:41:%SSA-5-FABRICSYNC_DONE:Fabric sync on Primary channel done.
Mar 25 16:40:41:%OIR-SP-6-INSCARD:Card inserted in slot 4, interfaces are now online
```

Related Commands

Command	Description
show hw-module all fpd	Displays the current versions of all FPDs for all of the supported card types on a router.
show hw-module slot fpd	Displays the current versions of all FPDs for a SIP in the specified slot location and for all of the SPAs installed in that SIP or any FPD-capable cards.
show hw-module subslot fpd	Displays the current versions of all FPDs for a particular SPA or all of the active SPAs on a router.
show upgrade fpd file	Displays the contents of an FPD image package file.
show upgrade fpd package default	Displays which FPD image package is needed for the router to properly support the SPAs or other FPD-capable cards.
show upgrade fpd progress	Displays the progress of the FPD upgrade while an FPD upgrade is taking place.
show upgrade fpd table	Displays various information used by the Cisco IOS software to manage the FPD image package file.
upgrade fpd auto	Configures the router to automatically upgrade the FPD image when an FPD version incompatibility is detected.
upgrade fpd path	Specifies the location from where the FPD image package should be loaded when an automatic FPD upgrade is initiated by the router.
upgrade hw-module subslot fpd file	Manually upgrades the current FPD image on the specified SPA.

upgrade hw-module subslot

Note The upgradehw-module subslot command is not available in Cisco IOS Release 12.2(33)SRB and later Cisco IOS 12.2SR releases. It is replaced by the upgrade hw-module subslot fpd file command.

Note The upgrade hw-module subslot command is not available in Cisco IOS Release 12.2(33)SB and later Cisco IOS 12.2SB releases. It is replaced by the upgrade hw-module subslot fpd file command.

Note The upgrade hw-module subslot command is not available in Cisco IOS Release 12.0(33)S2 and later Cisco IOS 12.0S releases. It is replaced by the upgrade hw-module subslot fpd file command.

To manually upgrade the current FPD image package on a SPA, use the **upgradehw-modulesubslot** command in privileged EXEC mode.

Cisco 7304
upgrade hw-module subslot *slot/subslot* **file** *file-url* [**reload**]

Cisco 7600 Series, Cisco 12000 Series
upgrade hw-module subslot *slot/subslot* **file** *file-url* [**force**]

Syntax Description

slot	Chassis slot number. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding “Identifying Slots and Subslots for SIPs and SPAs” topic in the platform-specific SPA software configuration guide.
subslot	Secondary slot number on a SPA interface processor (SIP) where a SPA is installed. Refer to the platform-specific SPA hardware installation guide and the corresponding “Specifying the Interface Address on a SPA” topic in the platform-specific SPA software configuration guide for subslot information.
file	Specifies that a file will be downloaded.
file-url	Specifies the location of the FPD image package file, beginning with the location or type of storage device (examples include disk0, slot0, tftp, or ftp) and followed by the path to the FPD image package file.
reload	(Optional) Reloads the SPA to complete the FPD upgrade.
force	(Optional) Forces the update of all compatible FPD images in the indicated FPD image package on the SPA that meet the minimal version requirements. Without this option, the manual upgrade will only upgrade incompatible FPD images.

Command Default

No default behavior or values, although it is important to note that the router containing the SPA is configured, by default, to upgrade the FPD images when it detects a version incompatibility between a the FPD image on the SPA and the FPD image required to run the SPA with the running Cisco IOS image. The **upgradehw-modulesubslot** command is used to manually upgrade the FPD images; therefore, the **upgradehw-modulesubslot**command should only be used when the automatic upgrade default configuration fails to find a compatible FPD image for one of the SPAs or when the automatic upgrade default configuration has been manually disabled. The **noupgradefpdauto** command can be entered to disable automatic FPD upgrades.

By default the SPA is not reloaded to complete the FPD upgrade unless the **reload** option is entered. Reloading the SPA drops all traffic traversing that SPA's interfaces. If you want to reload the SPA later to complete the upgrade, do not enter the **reload** option and perform OIR of the SPA later to complete the FPD upgrade.

If no FPD incompatibility is detected, this command will not upgrade SPA FPD images unless the **force** option is entered.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(20)S2	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(25)S3	The **force** option was removed and replaced by the **reload** option (Cisco 7304 router).
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was removed. It is not available in Cisco IOS Release 12.2(33)SRB and later Cisco IOS 12.2SR releases. It is replaced by the upgrade hw-module subslot fpd file command.
12.2(33)SB	This command was removed. It is not available in Cisco IOS Release 12.2(33)SB and later Cisco IOS 12.2SB releases. It is replaced by the upgrade hw-module slot fpd file command.

Usage Guidelines

This command is used to manually upgrade the FPD images on a SPA. In most cases, the easiest and recommended method of upgrading FPD images is the automatic FPD upgrade, which is enabled by default. The automatic FPD upgrade will detect and automatically upgrade all FPD images when an FPD incompatibility is detected.

A manual FPD upgrade is usually used in the following situations:

- The target SPA was disabled by the system because of an incompatible FPD image (the system could not find the required FPD image package file).
- A recovery upgrade must be performed.
- A special bug fix to an FPD image is provided in the FPD image package file.

The FPD image upgrade process places the SPA offline. The time required to complete an FPD image upgrade can be lengthy. The **showupgradeprogress** command can be used to gather more information about estimated FPD download times for a particular SPA.

For more information about FPD upgrades on SPA interface processors (SIPs) and shared port adapters (SPAs), see the *Cisco 7304 Router Modular Services Card and Shared Port Adapter Software Configuration Guide*, the *Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide*, or the *Cisco 12000 Series Router SIP and SPA Software Configuration Guide*.

Examples

The following example shows a sample manual FPD upgrade:

```
Router# upgrade hw-module subslot 2/0 file disk0:spa_fpd.122-20.S2.pkg
% Uncompressing the bundle ...  [OK]

% The following FPD(s) will be upgraded for card in subslot 2/0 :

         ================== =========== =========== ============
         Field Programmable   Current     Upgrade   Estimated
         Device:"ID-Name"     Version     Version   Upgrade Time
         ================== =========== =========== ============
         1-Data & I/O FPGA
     4.12        4.13      00:06:00
         ================== =========== =========== ============
% Are you sure that you want to perform this operation? [no]:y
% Restarting the target card (subslot 2/0) for FPD image upgrade. Please wait ...

Router#
*Jan 14 00:37:17:%FPD_MGMT-6-FPD_UPGRADE_TIME:Estimated total FPD image upgrade time for
SPA-4FE-7304 card in subslot 2/0 = 00:06:00.
*Jan 14 00:37:17:%FPD_MGMT-6-FPD_UPGRADE_START:4FE/2GE FPGA (FPD ID=1) image upgrade in
progress for SPA-4FE-7304 card in subslot 2/0. Updating to version 4.13. PLEASE DO NOT
INTERRUPT DURING THE UPGRADE PROCESS (estimated upgrade completion time = 00:06:00)
...[.........................(part of the output has been removed for brevity)....
...................................................................................]
SUCCESS - Completed XSVF execution.

*Jan 14 00:42:59:%FPD_MGMT-6-FPD_UPGRADE_PASSED:4FE/2GE FPGA (FPD ID=1) image upgrade for
SPA-4FE-7304 card in subslot 2/0 has PASSED. Upgrading time = 00:05:42.596
*Jan 14 00:42:59:%FPD_MGMT-6-OVERALL_FPD_UPGRADE:All the attempts to upgrade the required
FPD images have been completed for SPA-4FE-7304 card in subslot 2/0. Number of
successful/failure upgrade(s):1/0.
*Jan 14 00:42:59:%FPD_MGMT-5-CARD_POWER_CYCLE:SPA-4FE-7304 card in subslot 2/0 is being
power cycled for the FPD image upgrade to take effect.
```

Related Commands

Command	Description
show hw-module slot fpd	Displays the current versions of FPD image files for all of the active SIPs on a router.
show hw-module subslot fpd	Displays the FPD version on each SPA in the router.
show upgrade fpd file	Displays the contents of an FPD image package file.
show upgrade fpd package default	Displays which FPD image package is needed for the router to properly support the SPAs.
show upgrade fpd progress	Displays the progress of the FPD upgrade while an FPD upgrade is taking place.
show upgrade fpd table	Displays various information used by the Cisco IOS software to manage the FPD image package file.

Command	Description
upgrade fpd auto	Configures the router to automatically upgrade the FPD image when an FPD version incompatability is detected.
upgrade fpd path	Specifies the location from where the FPD image package should be loaded when an automatic FPD upgrade is initiated by the router.
upgrade hw-module slot	Manually upgrades the current FPD image on the specified SPA.

upgrade hw-module subslot fpd file

To manually upgrade the current FPD image package on a SPA, use the **upgradehw-modulesubslotfpdfile**command in privileged EXEC mode.

Cisco 7304 and Cisco uBR10012 Universal Broadband Router
upgrade hw-module subslot *slot/subslot* **fpd file** *file-url* [**reload**]

Cisco 7600 Series
upgrade hw-module subslot *slot/subslot* **fpd file** *file-url* [**force**]

Syntax Description

slot	Chassis slot number. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding “Identifying Slots and Subslots for SIPs and SPAs” topic in the platform-specific SPA software configuration guide.
subslot	Secondary slot number on a SPA interface processor (SIP) where a SPA is installed. Refer to the platform-specific SPA hardware installation guide and the corresponding “Specifying the Interface Address on a SPA” topic in the platform-specific SPA software configuration guide for subslot information.
file-url	Specifies the location of the FPD image package file, beginning with the location or type of storage device (examples include disk0, slot0, tftp, or ftp) and followed by the path to the FPD image package file.
reload	(Optional) Reloads the SPA to complete the FPD upgrade.
force	(Optional) Forces the update of all compatible FPD images in the indicated FPD image package on the SPA that meet the minimal version requirements. Without this option, the manual upgrade will only upgrade incompatible FPD images.

Command Default

No default behavior or values, although it is important to note that the router containing the SPA is configured, by default, to upgrade the FPD images when it detects a version incompatibility between a the FPD image on the SPA and the FPD image required to run the SPA with the running Cisco IOS image. Manual upgrade of FPD images is recommended only when the automatic upgrade default configuration fails to find a compatible FPD image for one of the SPAs, or when the automatic upgrade default configuration has been manually disabled. The **noupgradefpdauto** command can be entered to disable automatic FPD upgrades.

By default the SPA is not reloaded to complete the FPD upgrade unless the **reload** option is entered. Reloading the SPA drops all traffic traversing that SPA’s interfaces. If you want to reload the SPA later to complete the upgrade, do not enter the **reload** option and perform OIR of the SPA later to complete the FPD upgrade.

If no FPD incompatibility is detected, this command will not upgrade SPA FPD images unless the **force** option is entered.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SRB	This command was introduced. This command replaces the upgrade hw-module subslot command.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.

Usage Guidelines

This command is used to manually upgrade the FPD images on a SPA. In most cases, the easiest and recommended method of upgrading FPD images is the automatic FPD upgrade, which is enabled by default. The automatic FPD upgrade will detect and automatically upgrade all FPD images when an FPD incompatibility is detected.

A manual FPD upgrade is usually used in the following situations:

- The target SPA was disabled by the system because of an incompatible FPD image (the system could not find the required FPD image package file).
- A recovery upgrade must be performed.
- A special bug fix to an FPD image is provided in the FPD image package file.

The FPD image upgrade process places the SPA offline. The time required to complete an FPD image upgrade can be lengthy. The **showupgradeprogress** command can be used to gather more information about estimated FPD download times for a particular SPA.

For more information about FPD upgrades on SPA interface processors (SIPs) and shared port adapters (SPAs), see the *Cisco 7304 Router Modular Services Card and Shared Port Adapter Software Configuration Guide* or the*Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide* .

Examples

The following example shows a sample manual FPD upgrade:

```
Router# upgrade hw-module subslot 2/0 fpd file disk0:spa_fpd.122-20.S2.pkg
% Uncompressing the bundle ...  [OK]

% The following FPD(s) will be upgraded for card in subslot 2/0 :

         ================== =========== =========== ============
         Field Programmable   Current     Upgrade   Estimated
         Device:"ID-Name"     Version     Version   Upgrade Time
         ================== =========== =========== ============
         1-Data & I/O FPGA
     4.12        4.13      00:06:00
         ================== =========== =========== ============
% Are you sure that you want to perform this operation? [no]:y
% Restarting the target card (subslot 2/0) for FPD image upgrade. Please wait ...

Router#
*Jan 14 00:37:17:%FPD_MGMT-6-FPD_UPGRADE_TIME:Estimated total FPD image upgrade time for
SPA-4FE-7304 card in subslot 2/0 = 00:06:00.
*Jan 14 00:37:17:%FPD_MGMT-6-FPD_UPGRADE_START:4FE/2GE FPGA (FPD ID=1) image upgrade in
progress for SPA-4FE-7304 card in subslot 2/0. Updating to version 4.13. PLEASE DO NOT
INTERRUPT DURING THE UPGRADE PROCESS (estimated upgrade completion time = 00:06:00)
...[.........................(part of the output has been removed for brevity)....
..................................................................................]
SUCCESS - Completed XSVF execution.
```

```
*Jan 14 00:42:59:%FPD_MGMT-6-FPD_UPGRADE_PASSED:4FE/2GE FPGA (FPD ID=1) image upgrade for
SPA-4FE-7304 card in subslot 2/0 has PASSED. Upgrading time = 00:05:42.596
*Jan 14 00:42:59:%FPD_MGMT-6-OVERALL_FPD_UPGRADE:All the attempts to upgrade the required
FPD images have been completed for SPA-4FE-7304 card in subslot 2/0. Number of
successful/failure upgrade(s):1/0.
*Jan 14 00:42:59:%FPD_MGMT-5-CARD_POWER_CYCLE:SPA-4FE-7304 card in subslot 2/0 is being
power cycled for the FPD image upgrade to take effect.
```

Related Commands

Command	Description
show hw-module slot fpd	Displays the current versions of FPD image files for all of the active SIPs on a router.
show hw-module subslot fpd	Displays the FPD version on each SPA in the router.
show upgrade fpd file	Displays the contents of an FPD image package file.
show upgrade fpd package default	Displays which FPD image package is needed for the router to properly support the SPAs.
show upgrade fpd progress	Displays the progress of the FPD upgrade while an FPD upgrade is taking place.
show upgrade fpd table	Displays various information used by the Cisco IOS software to manage the FPD image package file.
upgrade fpd auto	Configures the router to automatically upgrade the FPD image when an FPD version incompatibility is detected.
upgrade fpd path	Specifies the location from where the FPD image package should be loaded when an automatic FPD upgrade is initiated by the router.
upgrade hw-module slot fpd file	Manually upgrades the current FPD image on the specified SPA.

upgrade hw-programmable

To perform a Complex Programmable Logic Device (CPLD) or Field-Programmable Gate Array (FPGA) upgrade on a Cisco ASR 1000 Series Router, use the **upgradehw-programmable** command in Privileged EXEC configuration mode.

upgrade hw-programmable [{**all** | **CPLD** | **FPGA**}] **filename** *filename* {**R0** | **R1** | **F0** | **F1** | **0 . . 5**}

Syntax Description

all	Select to perform both a CPLD and FPGA upgrades on a Cisco ASR 1000 Series Router. **Note** This option is not supported in Cisco IOS XE Release 3.1.0S.
CPLD	Select to perform a Complex Programmable Logic Device (CPLD) upgrade on the Cisco ASR1000-SIP10, standby or active Cisco ASR1000-RP in a Cisco ASR 1013 Router.
FPGA	Select to perform a Field-Programmable Gate Array (FPGA) upgrade on a Cisco ASR 1000 Series Router. **Note** This option is not supported in Cisco IOS XE Release 3.1.0S.
filename	Specifies the hw-programmable upgrade package file.
filename	Specifies the hw-programmable upgrade package file and its file system location. For filename, specify one of the following system locations and a package file name: • bootflash: RP-relative HW programmable package name • flash: RP-relative HW programmable package name • harddisk: RP-relative HW programmable package name This is the hw-programmable upgrade package file that contains a new version of the CPLD and FPGA code, used for performing the CPLD on a Cisco ASR 1013 Router or FPGA upgade on a Cisco ASR 1000 Series Router. The package file name is typically named asr1000-hw-programmables.<release_name>.pkg.
R0	RP slot 0. In the Cisco ASR 1006 Routers and Cisco ASR 1013 Routers, it is the lower RP slot. In the Cisco ASR 1002 and Cisco ASR 1004 Routers, it is the only slot.
R1	RP slot 1. This is only in the Cisco ASR 1006 and Cisco ASR 1013 Routers. It is the higher RP slot.
F0	This is the embedded services processor (ESP) slot 0. In the Cisco ASR 1006 Routers and Cisco ASR 1013 Routers, it is the lower ESP slot. In the Cisco ASR 1002 and Cisco ASR 1004 Routers, it is the only slot.
F1	This is the embedded services processor (ESP) slot 2. This is only in the Cisco ASR 1006 and Cisco ASR 1013 Routers. It is the higher ESP slot.

0..5	This is one of the SIP carrier card slots. Select a slot number zero through five. **Note** A CPLD upgrade cannot be performed in Slot 5 in the ASR100-SIP10. Move the card to another slot.

Command Default

CPLD or FPGA is not upgraded.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced in Cisco IOS XE Release 3.1S.

Usage Guidelines

For procedures on performing a CPLD upgrade, see the Upgrading Field Programmable Hardware Devices for Cisco ASR 1000 Series Routers document.

Examples

The following example upgrades the Cisco ASR1000-RP2 CPLD with the following command:

```
Router# upgrade hw-programmable cpld filename harddisk: asr1000-hw-programmables.15.01s.pkg
 R0
Upgrade CPLD on Route-Processor 0 from current version 08103002 to 10021901 [confirm] This
 command could take up to 10 minutes, please wait and do not power cycle the box or the
card (hardware may be unrecoverable). This command  also issues a reset to the linecard at
 the end of upgrade.[confirm]
```

Related Commands

Command	Description
show hw-programmable	Displays the current CPLD and FPGA versions on a Cisco ASR 1000 Series Router.
show upgrade hw-programmable progress	Displays the upgrade progress of the line card-field upgradeable device (LC-FPD) on a Cisco ASR 1000 Series Router.
show upgrade hw-programmable	Displays the names and versions of individual files in the hw_programmable package file.

upgrade rom-monitor default

To configure a particular ROM monitor image as the default ROMmon image, use the **upgraderom-monitordefault** command in privileged EXEC mode.

upgrade rom-monitor {**rom0** | **rom1** | **rom2**} **default**

Syntax Description

rom0	One-time programmable, always-there "golden" ROMmon.
rom1	Upgradable ROM monitor 1.
rom2	Upgradable ROM monitor 2.

Command Default

ROM 0, the one-time programmable, always there "golden" ROMmon is the default ROM monitor.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(9)EX	This command was introduced.
12.2(18)S	This command was implemented on Cisco 7304 routers running Cisco IOS Release 12.2 S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to set a ROMmon image as the default ROMmon image. If this command is not configured, the system uses ROM 0 as the default ROMmon image.

There are three ROMmon images. ROM 0 is a one-time programmable, always-there ROMmon image, referred to as the "golden" ROMmon. ROM 1 and ROM 2 are upgradeable ROMmon images. At bootup, the system uses the golden ROMmon by default. If either ROM 1 or ROM 2 are configured, the system still begins bootup with the golden ROMmon, then switches to the configured ROMmon. If a new configured ROMmon image fails to boot up Cisco IOS, the router marks this ROMmon image as invalid and reverts to the golden image for the next Cisco IOS bootup.

After downloading a new ROMmon image to the writeable ROMmon, you must reload Cisco IOS for the new ROMmon to take effect. The first time a new ROMmon image is loaded, you must allow the system to boot up Cisco IOS before doing any resets or power cycling. If the ROMmon loading process is interrupted, the system interprets this as a bootup failure of the new ROMmon image and reverts the ROMmon back to the golden ROMmon image in ROM 0.

Examples

The following example configures ROM 2 as the default ROMmon image:

```
Router# upgrade rom-monitor rom2 default
done!
Will take effect on next reload/reset
```

Related Commands

Command	Description
show c7300	Displays the types of hardware installed in a Cisco 7304 router.
show platform	Displays the platform.
show diag	Displays hardware information for any slot or the chassis.
upgrade rom-monitor file	Upgrades the ROM monitor.

upgrade satellite satellite

To upgrade the firmware of an NM-1VSAT-GILAT network module through TFTP, use the **upgradesatellitesatellite** command in privileged EXEC mode.

upgrade satellite satellite *slot/unit tftp-server-address firmware-filename*

Syntax Description

slot/	Router chassis slot in which the network module is installed. The / must be typed in between *slot* and *unit*.
unit	Interface number. For NM-1VSAT-GILAT network modules, always use 0.
tftp-server-address	The IP address of the TFTP server that contains the firmware upgrade.
firmware-filename	The name of the file with the upgraded firmware.

Command Default

Firmware will not be upgraded through TFTP.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(11)XJ2	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

The **upgradesatellitesatellite** command is used to provide a firmware upgrade of VSATs locally at remote sites through TFTP. This method reduces dependency on a central hub, and allows for ease of update when connected to a service provider who uses third-party hubs.

When the TFTP server is configured on the router, the VSAT firmware is copied to the router flash memory. The TFTP server configuration would be as follows:

```
tftp-server flash:< <firmware filename>
```

This configuration would be within the overall router configuration.

When this configuration is done, the upgrade is accomplished by pointing the VSAT to the router IP address in the **upgradesatellitesatellite** command. The upgrade process will take several minutes.

Examples

The following example shows the response of the NM-1VSAT-GILAT network module to a firmware upgrade command.

```
Router# upgrade satellite satellite 1/0 9.1.0.1 VSAT_99.06.01.26_Bin.bin

Download of new firmware will proceed after a reboot of
 the satellite network module. This could take up to two minutes.
 Please wait...


*Mar 4 03:18:15.006: %LINEPROTO-5-UPDOWN: Line protocol on Interface Satellite1/0, changed
```

```
 state to up
The upgrade process will complete in several minutes.
 It will take place in the background.
 Please monitor the console for errors.
*Mar 4 03:21:16.006: %LINEPROTO-5-UPDOWN: Line protocol on Interface Satellite1/0, changed
 state to down
*Mar 4 03:27:20.842: %LINEPROTO-5-UPDOWN: Line protocol on Interface Satellite1/0, changed
 state to up
```

Related Commands

Command	Description
service-module satellite status	Verifies the image version of the downloaded firmware.

utc offset leap-second offset

To configure the current UTC offset, leap second event date and Offset value (+1 or -1), use the **utc offset leap-second offset** command in PTP clock configuration mode.

utc offset *value* **leap-second** *"date time"* **offset** {**-1** | **1**}

Syntax Description

value	Current UTC offset value. Valid values are from 0-255. The default value is 36.
"date time"	Leap second effective date in dd-mm-yyyy hh:mm:ss format.

Command Default

By default no UTC offset or leap second is configured.

Command Modes

PTP clock configuration (config-ptp-clk)

Command History

Release	Modification
Cisco IOS XE 3.18SP	This command was introduced.
Cisco IOS XE 3.18.1SP	This command was modified. The **leap-second** and **offset** keywords were added.

Usage Guidelines

Use the **utc offset leap-second offset** command to configure the current UTC offset, leap second event date and Offset value (+1 or -1).

The following example shows how to configure the current UTC offset, leap second event date and offset value:

```
Device(config)# ptp clock boundary domain 0 hybrid
Router(config-ptp-clk)# time-properties persist 600
Router(config-ptp-clk)#utc-offset 45 leap-second "01-01-2017 00:00:00" offset 1
```

Related Commands

Command	Description
time-properties persist	Configures time properties holdover time.

vectoring

To enable the vectoring mode in C86xVAE platforms, use the **vectoring** command in controller configuration mode. To restore the default value, use the **no** form of this command.

vectoring {friendly | none}

no vectoring

Syntax Description

friendly	Enables friendly vectoring mode in both Annex A and Annex B.
none	Disables vectoring mode completely.

Command Default

Default mode is Vectoring friendly in Annex A and Annex B from Release 15.6(3)M.

Command Modes

Controller Configuration (config-controller)

Command History

Release	Modification
15.6(3)M	This command was introduced on the Cisco C86xVAE series routers.

Usage Guidelines

This command is used to enable or disable vectoring on C867VAE-K9 and C866VAE-K9 platforms. By default, the vectoring is friendly on both annex A and Annex B. This command is introduced under "controller vdsl 0" mode.

Examples

The following example shows how to enable vectoring :

```
Router(config-controller)#vectoring friendly
```

The following example shows how to disable vectoring :

```
Router(config-controller)#vectoring none
```

Related Commands

Command	Description
controller vdsl	Configures the controller status.

vtg

To configure the Circuit Emulation Services over Packet Switched Network (CESoPSN) CEM group, use the **vtg** command in controller configuration STS mode.

vtg *vtg_number* **t1** *t1_line_number* **cem-group** *channel-number* **timeslots** *list-of-timesolts*

Syntax Description

For NCS 4200 Series Routers:

vtg *vtg-number* **vt** *vt-line-number* **cem-group** *cem-group-number* **cep**

vtg_number	Specifies the VTG number. The range is 1 to 7.
t1	Specifies the T1 line configuration.
t1_line_number	Specifies the T1 line number. The range is 1 to 4.
cem-group	Specifies the timeslots to CEM group mapping.
channel-number	Specifies the channel number. The range is 0 to 2015.
timeslots	Specifies the timeslots in the CEM group.
list-of-timesolts	Specifies the list of timeslots. The range is 1 to 24
vt	Specifies the Virtual Tributary (VT) under vtg of STS.
vt-line-number	Specifies the VT line number.
cem-group	Specifies the CEM group for T1 line.
cem-group-number	The *cem-group-number* keyword identifies the channel number to be used for this channel. For T1 ports, the range is 0 to 23. For E1 ports, the range is 0 to 30.
cep	Configures Circuit Emulation Service over Packet (CEP) mode.

Command Default

None

Command Modes

Controller configuration STS

Command History

Release	Modification
15.1(01)S	This command was introduced on the Cisco 7600 routers.
XE 3.18 SP	Support for this command was introduced on NCS 4200 Series.

Examples

This example shows how to configure the (CESoPSN) CEM group:

```
Router(config)# controller sonet-acr 1
```

```
Router(config-controller)#
sts-1 2
Router (config-ctrlr-sts1)#vtg 2 T1 2 cem-group 2 timeslots 2
```

Examples

For NCS 4200 Series, this command is used to configure the VT-15 CEP mode:

```
enable
configure terminal
controller Mediatype 0/5/0
controller sonet 0/5/0
sts-1 1
vtg 1 vt 1 cem-group 100 cep
end
```

Related Commands

Command	Description
sts-1	Configures the Synchronous Transport Signal (STS) (level)-1 in the SONET hierarchy.
mode vt-15	Configures the path operation mode.
controller sonet-acr	Configures the SONET Access Circuit Redundancy (ACR) virtual controller.
show controller sonet	Displays SONET controller configuration.

wanphy flag j1 transmit

T o configure the J1 byte values on the local SPA and to check the connectivity to the remotely connected SPA by passing the J1 byte values, use the **wanphyflagj1transmit***byte-value*commandin the Controller configuration mode. To deconfigure the J1 byte value and stop the J1 byte value from being sent to the remote end, use the **no** form of this command.

wanphy flag j1 transmit *byte-value*
no wanphy flag j1 transmit

Syntax Description

byte-value	J1 byte value that is sent from the local SPA to the remote SPA. Length of string in bytes. The range is from 0 to 16 bytes.
j1	Specifies that the J1 byte value is passed from the local SPA to the remote SPA.
transmit	Transmits the specified byte value passed from the local SPA to the remote SPA.

Command Default

No default behavior or values are available.

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
Cisco IOS XE Release 3.3.0S	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines

The **wanphyflagj1transmit**command has been has been introduced on the Cisco ASR 1000 Series Routers in Cisco IOS XE Release 3.3.0S. The main purpose of this command is to pass a J1 string value from the local Cisco 1-Port 10 Gigabit Ethernet LAN/WAN-PHY Shared Port Adapter to the remote SPA in order to check the connectivity between the two SPAs.

Note Both the local and remotely connected Cisco 1-Port 10 Gigabit Ethernet LAN/WAN-PHY Shared Port Adapter must operate in the WAN mode.

Examples

The following example shows how to pass a J1 byte value string from locally installed SPA to a remote SPA:

```
Router# config
Router(config)# controller wanphy 2/1/0
Router(config-controller)# wanphy flag j1 transmit messagefromlocalspa
```

Related Commands

Command	Description
show controllers wanphy	Displays the SPA mode (LAN mode or WAN mode), alarms, and the J1 byte string value.

wanphy report-alarm

T o enable selective alarm reporting for line-level, path-level, or section-level alarms, use the **wanphyreport-alarm**commandin Controller configuration mode. To reset the alarm reporting to its default, use the **no** form of this command.

wanphy report-alarm {*defaultlinepathsectionwis*}
no wanphy threshold

Syntax Description

default	Alarm reporting of line, section, and path to their default configured values.
line	The line-level alarm reporting status.
path	The path-level alarm reporting status.
section	The section-level alarm reporting status.
wis	The WIS-level alarm reporting status.

Command Default

No default values are available.

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
Cisco IOS XE Release 3.3.0S	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines

The **wanphyreport-alarm**command has been introduced on the Cisco ASR 1000 Series Routers in Cisco IOS XE Release 3.3.0S. The main purpose of this command is to selectively add more line-level, section-level, WIS-level, and path-level alarms over and above the default configured alarms. To set alarm reporting to its default value, use the **nowanphyreport-alarm** command.

Examples

The following example shows how to configure the line-level alarms:

```
Router# config
Router(config)# controller wanphy 2/1/0
Router(config-controller)# wanphy report-alarm line
```

The following example shows how to configure the path-level alarms:

```
Router# config
Router(config)# controller wanphy 2/1/0
Router(config-controller)# wanphy report-alarm path
```

The following example shows how to configure the section-level alarms:

```
Router# config
Router(config)# controller wanphy 2/1/0
Router(config-controller)# wanphy report-alarm section
```

The following example shows how to configure the WIS-level alarms:

```
Router# config
Router(config)# controller wanphy 2/1/0
Router(config-controller)# wanphy report-alarm wis
```

The following example shows how to reconfigure the alarms to their default values:

```
Router# config
Router(config)# controller wanphy 2/1/0
Router(config-controller)# wanphy report-alarm default
```

Related Commands

Command	Description
show controllers wanphy	Displays the SPA mode (LAN mode or WAN mode), alarms, and the J1 byte string value.

wanphy threshold

T o configure the physical layer threshold values for b1-tca, b2-tca, the Signal Degrade (SD) Bit Error Rate (BER), and Signal Failure (SF) BER, use the **wanphythreshold**commandin the Controller configuration mode. To reset the threshold alarm values to its default values, use the **no** form of the command.

wanphy threshold {*b1-tcab2-tcasd-bersf-ber*}
no wanphy threshold

Syntax Description

b1-tca	The B1 BER threshold-crossing alarm value. The default b1-tca value is 10e-6. The valid range is 4 to 9.
b2-tca	The B2 BER threshold-crossing alarm values. The default b2-tca value is 10e-6. The valid range is 3 to 9.
sd-ber	The SD BER threshold-crossing alarm value. The range value is expressed exponentially as 10e-n. The default sd-ber value is 6 (10e-6). The valid range is 3 to 9.
sf-ber	The SF BER threshold-crossing alarm value. The range value is expressed exponentially as 10e-n. The default sf-ber value is 3 (10e-3). The valid range is 3 to 9.

Command Default

By default, SF-BER, SD-BER, B1-tca, and B2-tca are enabled. However, alarm logging is enabled only for SF-BER.

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
Cisco IOS XE Release 3.3.0S	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines

The **wanphythreshold**command has been introduced on the Cisco ASR 1000 Series Routers in Cisco IOS XE Release 3.3.0S. The main purpose of this command is to configure the threshold values for SF-BER and SD-BER.

Examples

The following example shows how to configure the B1 TCA value:

```
Router# config
Router(config)# controller wanphy 2/1/0
Router(config-controller)# wanphy threshold b1-tca 4
```

The following example shows how to configure the B2 TCA value:

```
Router# config
Router(config)# controller wanphy 2/1/0
Router(config-controller)# wanphy threshold b2-tca 5
```

The following example shows how to configure the SD-BER threshold value:

```
Router# config
```

```
Router(config)# controller wanphy 2/1/0
Router(config-controller)# wanphy threshold sd-ber 8
```

The following example shows how to configure the SF-BER threshold value:

```
Router# config
Router(config)# controller wanphy 2/1/0
Router(config-controller)# wanphy threshold sf-ber 9
```

Related Commands

Command	Description
show controllers wanphy	Displays the SPA mode (LAN mode or WAN mode), alarms, and the J1 byte string value.

xconnect (CEM)

To build one end of a circuit emulation (CEM) connection and to enter CEM xconnect configuration mode, use the **xconnect** command in CEM configuration mode. To remove any existing CEM connections from this CEM channel, use the **no** form of this command.

xconnect *remote-ip-address* *virtual-connect-ID* **encapsulation** *encapsulation-type*
no xconnect

Syntax Description

remote-ip-address	IP address of an interface--physical or loopback--on the destination router.
virtual-connect-ID	Virtual connect ID (VCID). For CEM over IP (CEoIP), you must enter a value of 0.
encapsulation	Sets the encapsulation type.
encapsulation-type	Encapsulation type. You must set the encapsulation type to UDP. For Cisco NCS 4200 Series, you must set the encapsulation type to mpls.

Command Default

No CEM connections are built.

Command Modes

CEM configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
XE 3.18SP	This command was implemented on the Cisco NCS 4200 Series.
XE 3.18.1SP	This command was implemented on the Cisco ASR 900 Series Routers.
XE Everest 16.5.1	This command was implemented on the Cisco ASR 920 Routers.

Examples

The following example shows how to build one end of a CEoIP connection and to enter CEM xconnect configuration mode.

```
Router(config-cem)# xconnect 10.0.5.1 0 encapsulation udp
Router(config-cem-xconnect)#
```

Examples

The following example shows how to enter CEM xconnect configuration mode.

```
Router(config-if-cem)# xconnect 10.10.10.10 200 encapsulation mpls
Router(config-if-xconnect)#
```

Related Commands

Command	Description
cem	Enters circuit emulation configuration mode.

Command	Description
local ip address	Defines the IP address of the local router.
local udp port	Defines the local UDP port.
remote udp port	Defines the UDP port of a remote endpoint.
show cem	Displays CEM channel statistics.

yellow

To enable generation and detection of yellow alarms, use the **yellow** command in interface configuration mode.

yellow {**generation** | **detection**}

Syntax Description

generation	Enables or disables generation of yellow alarms.
detection	Enables or disables detection of yellow alarms.

Command Default

Yellow alarm generation and detection are enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)XE	This command was introduced.
12.0(7)XE1	This command was implemented on Cisco 7100 series routers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to generate and detect yellow alarms. If the received signal is lost the yellow alarm can be generated to indicate a frame loss event. Generation of a yellow alarm will ensure that the alarm is sent to the remote end of the link. When the remote end is transmitting a yellow alarm, detection must be enabled to detect the alarm condition.

Examples

The following example shows how to enable generation and detection of yellow alarms on a Cisco 7500 series router:

```
Router
(config)
# interface atm 3/1/0
Router
(config-if)
# yellow generation
Router
(config-if)
# yellow detection
```