



Cisco Nexus 7000 Series NX-OS Interfaces Command Reference

First Published: 2016-11-24

Last Modified: 2019-03-01

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

PREFACE

Preface	xiii
Preface	xiii
Audience	xiii
Document Conventions	xiii
Related Documentation	xiv
Documentation Feedback	xv
Communications, Services, and Additional Information	xv

CHAPTER 1

A Commands	1
action	2
auto-recovery	3

CHAPTER 2

B Commands	5
bandwidth (interface)	6
bfd	8
bfd authentication	9
bfd c-bit	11
bfd echo	12
bfd interval	14
bfd multihop authentication	16
bfd multihop hosting-linecard	17
bfd multihop interval	18
bfd optimize subinterfaces	20
bfd per-link	21
bfd slow-timer	23

CHAPTER 3**C Commands 25**

- capabilities-conflict 26
- carrier-delay 28
- channel-group 30
- clear counters interface 34
- clear l2protocol tunnel counters 36
- clear lacp counters 37
- clear vpc statistics 38
- config-sync 39
- connection timeout 40
- critical-event 42

CHAPTER 4**D Commands 45**

- default interface 46
- delay 47
- delay restore 48
- delay restore interface-vlan 49
- delay restore interface-vlan batch 50
- description 51
- discovery-timeout 52
- dual-active exclude interface-vlan 54
- duplex 55
- dying-gasp 56

CHAPTER 5**E Commands 59**

- encapsulation dot1Q 60
- errdisable detect cause 61
- errdisable recovery cause 62
- errdisable recovery interval 64
- ethernet oam 65
- ethernet oam profile 66

CHAPTER 6**F Commands 67**

fabricpath switch-id	68
feature bfd	69
feature ethernet-link-oam	70
feature interface-vlan	71
feature lacp	72
feature tunnel	73
feature udd	74
feature vpc	75
fec	76
flowcontrol	78
frame-period threshold	80
frame-period window	81
frame-seconds threshold	82
frame-seconds window	84
frame threshold	85
frame window	87

CHAPTER 7**G Commands** 89

graceful consistency-check	90
----------------------------	----

CHAPTER 8**H Commands** 91

high-threshold	92
hsrp bfd	94

CHAPTER 9**I Commands** 95

inherit port-profile	96
interface cmp-mgmt module	98
interface ethernet	99
interface loopback	100
interface mgmt	101
interface port-channel	102
interface tunnel	104
interface vlan	105
ip eigrp bfd	106

ip ospf bfd 107
ip pim bfd-instance 108
ip pim bfd 109
ipv6 eigrp bfd 110
isis bfd 111

CHAPTER 10**L Commands 113**

l2protocol tunnel 114
l2protocol tunnel cos 115
l2protocol tunnel drop-threshold 116
l2protocol tunnel shutdown-threshold 117
lACP graceful-convergence 118
lACP max-bundle 120
lACP min-links 121
lACP port-priority 122
lACP rate 123
lACP suspend-individual 124
lACP system-priority 126
layer3 peer-router 127
link-monitoring 128
link debounce 129
link-monitor 131
load-interval 132

CHAPTER 11**M Commands 135**

max-ports 136
mdix auto 137
medium 138
mode auto 139
mode (Ethernet OAM) 140
mode (require-remote) 141
mtu 142

CHAPTER 12**O Commands 143**

ospfv3 bfd 144

CHAPTER 13**P Commands 145**

peer-gateway 146
peer-keepalive destination 147
peer-switch 151
port-channel limit 152
port-channel load-balance 154
port-channel load-balance hash-modulo 156
port-channel load-defer 157
port-profile 158
profile (EOAM) 161

CHAPTER 14**R Commands 163**

rate-mode dedicated 164
rate-mode shared 166
reload restore 167
remote-loopback disable 168
role priority 169
router ospfv3 170

CHAPTER 15**S Commands 171**

self-isolation 172
session-down 173
session-up 175
shutdown 176
shutdown lan 177
speed 178
state enabled 180
switchport 181
switchport access vlan 182
switchport autostate exclude 183
switchport dot1q ethertype 184
switchport host 185

switchport mode	186
switchport mode dot1q-tunnel	188
switchport trunk allowed vlan	189
switchport trunk native vlan	191
switchport trunk native vlan tag	192
symbol-period threshold	194
symbol-period window	195
system-mac	196
system-priority	197
system default interface congestion mode	198
system default interface congestion timeout	199
system default interface pause mode	201
system default interface pause timeout	202
system default link-fail laser-on	203
system default switchport	204
system jumbomtu	205
system module-type	206

CHAPTER 16**Show Commands 207**

show bfd neighbors	209
show cfs application	213
show errdisable	215
show ethernet oam configuration	217
show ethernet oam discovery	219
show ethernet oam event-log	221
show ethernet oam statistics	223
show ethernet oam summary	225
show interface	227
show interface brief	229
show interface capabilities	231
show interface counters	233
show interface counters brief	236
show interface counters errors	239
show interface counters storm-control	243

show interface counters trunk	245
show interface debounce	246
show interface description	248
show interface ethernet	250
show interface flowcontrol	253
show interface mgmt	255
show interface port-channel	257
show interface port-channel counters	260
show interface status	264
show interface switchport	267
show interface transceiver	269
show interface trunk	271
show interface tunnel	273
show ip dhcp snooping statistics	274
show lacp counters	275
show lacp interface	276
show lacp neighbor	278
show lacp port-channel	279
show lacp summary	280
show lacp system-identifier	282
show ospfv3	283
show port-channel compatibility-parameters	285
show port-channel database	287
show port-channel load-balance	289
show port-channel rbh-distribution	290
show port-channel summary	291
show port-channel traffic	293
show port-channel usage	294
show port-profile	295
show running-config bfd	297
show running-config interface	298
show running-config interface mgmt	300
show running-config vpc	301
show running-config vpc-config-sync	302

[show startup-config interface](#) 303
[show startup-config vpc](#) 305
[show uddl](#) 306
[show vdc](#) 307
[show vpc brief](#) 308
[show vpc config-sync](#) 312
[show vpc consistency-parameters](#) 315
[show vpc orphan-ports](#) 318
[show vpc peer-keepalive](#) 320
[show vpc role](#) 322
[show vpc statistics](#) 324

CHAPTER 17
T Commands 325

[track](#) 326
[tunnel destination](#) 328
[tunnel mode](#) 329
[tunnel path-mtu-discovery](#) 330
[tunnel source](#) 332
[tunnel ttl](#) 333
[tunnel use-vrf](#) 334

CHAPTER 18
U Commands 335

[uddl](#) 336
[uddl aggressive](#) 337
[uddl message-time](#) 338
[uddl reset](#) 339
[uni-directional link-fault](#) 340

CHAPTER 19
V Commands 343

[vlan dot1q tag native](#) 344
[vpc](#) 346
[vpc config-sync re-merge](#) 347
[vpc domain](#) 349
[vpc orphan-ports suspend](#) 350

vpc peer-link 351

vpc sync 352

CHAPTER 20

W Commands 353

wiring-conflict 354



Preface

- [Preface, on page xiii](#)

Preface

This preface describes the audience, organization, and conventions of the Book Title. It also provides information on how to obtain related documentation.

This chapter includes the following topics:

Audience

This publication is for experienced network administrators who configure and maintain Cisco NX-OS on Cisco Nexus 7000 Series Platform switches.

Document Conventions



Note

- As part of our constant endeavor to remodel our documents to meet our customers' requirements, we have modified the manner in which we document configuration tasks. As a result of this, you may find a deviation in the style used to describe these tasks, with the newly included sections of the document following the new format.
- The Guidelines and Limitations section contains general guidelines and limitations that are applicable to all the features, and the feature-specific guidelines and limitations that are applicable only to the corresponding feature.

Command descriptions use the following conventions:

Convention	Description
bold	Bold text indicates the commands and keywords that you enter literally as shown.
<i>Italic</i>	Italic text indicates arguments for which the user supplies the values.

Convention	Description
[x]	Square brackets enclose an optional element (keyword or argument).
[x y]	Square brackets enclosing keywords or arguments separated by a vertical bar indicate an optional choice.
{x y}	Braces enclosing keywords or arguments separated by a vertical bar indicate a required choice.
[x {y z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
<i>variable</i>	Indicates a variable for which you supply values, in context where italics cannot be used.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Examples use the following conventions:

Convention	Description
<code>screen font</code>	Terminal sessions and information the switch displays are in screen font.
boldface screen font	Information you must enter is in boldface screen font.
<i>italic screen font</i>	Arguments for which you supply values are in italic screen font.
<>	Nonprinting characters, such as passwords, are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

This document uses the following conventions:



Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.



Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Documentation

Documentation for Cisco Nexus 7000 Series Switches is available at:

- Configuration Guides

<http://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/products-installation-and-configuration-guides-list.html>

- Command Reference Guides

<http://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/products-command-reference-list.html>

- Release Notes

<http://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/products-release-notes-list.html>

- Install and Upgrade Guides

<http://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/products-installation-guides-list.html>

- Licensing Guide

<http://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/products-licensing-information-listing.html>

Documentation for Cisco Nexus 7000 Series Switches and Cisco Nexus 2000 Series Fabric Extenders is available at the following URL:

<http://www.cisco.com/c/en/us/support/switches/nexus-2000-series-fabric-extenders/products-installation-and-configuration-guides-list.html>

Documentation Feedback

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at [Cisco Profile Manager](#).
- To get the business impact you're looking for with the technologies that matter, visit [Cisco Services](#).
- To submit a service request, visit [Cisco Support](#).
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit [Cisco Marketplace](#).
- To obtain general networking, training, and certification titles, visit [Cisco Press](#).
- To find warranty information for a specific product or product family, access [Cisco Warranty Finder](#).

Cisco Bug Search Tool

[Cisco Bug Search Tool](#) (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.



A Commands

- [action](#), on page 2
- [auto-recovery](#), on page 3

action

To enter the action configuration submode to configure what action is taken on an interface when a particular event occurs, use the **action** command in Ethernet OAM configuration mode or interface Ethernet OAM configuration mode.

action

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Ethernet OAM configuration (config-eoam)
Interface Ethernet OAM configuration (config-if-eoam)

Command History	Release	Modification
	7.3(0)D1(1)	This command was introduced.

Usage Guidelines This command does not require a license.

The following example shows how to enter the action configuration submode:

```
switch# configure terminal
switch(config)# ethernet oam profile Profile_1
switch(config-eoam)# action
switch(config-eoam-action)#
```

Related Commands

Command	Description
ethernet oam profile	Creates an EOAM profile and enters EOAM configuration mode.

auto-recovery

To configure the virtual port channel (vPC) for auto recovery if its peer is presumed nonoperational, use the **auto-recovery** command. To reset the vPC to the standard behavior, use the no form of this command.

auto-recovery reload-delay *time-out-value*
no auto-recovery reload-delay *time-out-value*

Syntax Description	reload-delay	Specifies the duration to wait after reload to recovery vPCs.
	<i>time-out-value</i>	Timeout value for restoring vPC links in seconds. The range is from 240 to 3600.

Command Default None

Command Modes VPC domain configuration mode (config-vpc-domain)

Command History	Release	Modification
	5.2(1)	This command was introduced.

Usage Guidelines This command does not require a license.

Examples This example shows how to configure the vPC for auto recovery:

```
switch# configure terminal
switch(config)# vpc domain 1
switch(config-vpc-domain)# auto-recovery reload-delay 350
Warning:
  Enables restoring of vPCs in a peer-detached state after reload, will wait for
  350 seconds to determine if peer is un-reachable
switch(config-vpc-domain)#
```

This example shows how to revert the vPC to the standard behavior:

```
switch# configure terminal
switch(config)# vpc domain 1
switch(config-vpc-domain)# no auto-recovery reload-delay 350
switch(config-vpc-domain)#
```

Related Commands	Command	Description
	vpc	Moves other port channels into the vPC.
	vpc domain	Creates a vPC domain.



B Commands

- [bandwidth \(interface\)](#), on page 6
- [bfd](#), on page 8
- [bfd authentication](#), on page 9
- [bfd c-bit](#), on page 11
- [bfd echo](#), on page 12
- [bfd interval](#), on page 14
- [bfd multihop authentication](#), on page 16
- [bfd multihop hosting-linecard](#), on page 17
- [bfd multihop interval](#), on page 18
- [bfd optimize subinterfaces](#), on page 20
- [bfd per-link](#), on page 21
- [bfd slow-timer](#), on page 23

bandwidth (interface)

To set the inherited and received bandwidth values for an interface, use the **bandwidth** command. To restore the default values, use the **no** form of this command.

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

Syntax Description

<i>kbps</i>	Intended bandwidth, in kilobits per second. The range is from 1 to 10000000.
inherit	(Optional) Specifies the inherited bandwidth such as how a subinterface inherits the bandwidth of its main interface.

Command Default

1000000 kbps

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

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

The **bandwidth inherit** command controls how a subinterface inherits the bandwidth of its main interface.

The **no bandwidth inherit** command enables all subinterfaces to inherit the default bandwidth of the main interface, regardless of the configured bandwidth. If a bandwidth is not configured on a subinterface, and you use the **bandwidth inherit** command, all subinterfaces inherit the current bandwidth of the main interface. If you configure a new bandwidth on the main interface, all subinterfaces use this new value.

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

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

This command does not require a license.

Examples

This example shows how to configure all subinterfaces off this main interface to inherit the configured bandwidth:

```
switch(config-if)# bandwidth inherit 30000
```

Related Commands

Command	Description
show interface	Displays the interface configuration information.

bfd

To enable Bidirectional Forwarding Detection (BFD) for a protocol, use the **bfd** command. To disable BFD for a protocol, use the **no** form of this command.

bfd
no bfd

Syntax Description

This command has no arguments or keywords.

Command Default

BFD is not enabled on the protocol.

Command Modes

Router configuration mode Neighbor configuration mode

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

There are two methods to configure protocols to use BFD for failure detection. To enable BFD for all neighbors or interfaces of a protocol, enter the **bfd** command in router configuration mode for the Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPFv2), Open Shortest Path First (OSPFv3) and Intermediate-System-to-Intermediate-System (IS-IS) or in neighbor configuration mode for the Border Gateway Protocol (BGP). If you do not want to enable BFD on all interfaces, see the interface-level BFD enable commands in the Related Commands section.

Examples

This example shows how to enable BFD for all EIGRP neighbors:

```
switch# configure terminal
switch(config)# router eigrp Test1
switch(config-router)# bfd
```

This example shows how to enable BFD for all BGP neighbors:

```
switch# configure terminal
switch(config)# router bgp 1.1
switch(config-router)# neighbor 192.0.2.1 remote-as 1.0
switch(config-router-neighbor)# bfd
```

Related Commands

Command	Description
hsrp bfd	Enables BFD on an HSRP interface.
ip eigrp bfd	Enables BFD on an EIGRP interface.
ip ospf bfd	Enables BFD on an OSPFv2 interface.
isis bfd	Enables BFD on an IS-IS interface.

bfd authentication

To configure SHA-1 authentication for all Bidirectional Forwarding Detection (BFD) sessions on the interface, use the `bfd authentication` command. To remove the SHA-1 authentication configuration, use the `no` form of this command.

bfd [**{ipv4 | ipv6}**] **authentication keyed-SHA1 key-id** *id* *hex-key* **key** *ascii-key*
no bfd [**{ipv4 | ipv6}**] **authentication keyed-SHA1 key-id** *id* *hex-key* **key** *ascii-key*

Syntax Description	Parameter	Description
	ipv4	(Optional) Enables BFD authentication for the IPv4 address.
	ipv6	(Optional) Enables BFD authentication for the IPv6 IP address.
	key-id	Specifies the key ID to use in BFD frames.
	<i>id</i>	Key ID value. The range is from 1 to 255.
	<i>hex-key</i>	HEX binary SHA1 secret. A hex-key can be any case-sensitive, alphanumeric string up to 40 characters.
	key	Specifies the ASCII SHA1 secret.
	<i>ascii-key</i>	SHA1 secret value. An ASCII key can be any case-sensitive, alphanumeric string up to 20 characters.

Command Default None

Command Modes Interface configuration mode (config-if)

Command History	Release	Modification
	6.2(2)	Added ipv4, ipv6 keywords to the syntax description.
	5.2(1)	This command was introduced.

Usage Guidelines This command does not require a license.

Examples

This example shows how to configure SHA-1 authentication for all BFD sessions on the interface:

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# bfd authentication keyed-SHA1 key-id 23 key cisco123
switch(config-if)#
```

This example shows how to disable SHA-1 authentication on the interface:

```
switch(config-if)# no bfd authentication keyed-SHA1 key-id 23 key cisco123
switch(config-if)#
```

Related Commands	Command	Description
	show running-config bfd	Displays the BFD running configuration.

Command	Description
show running-config interface	Displays the running configuration for a specific interface.

bfd c-bit

To configure the control plane independent bit setting in outgoing BFD packets, use the **bfdc-bit** command. To remove the control plane independent bit setting configuration, use the **no** form of this command.

bfdc-bit
nobfdc-bit

Syntax Description

This command has no keywords or arguments.

Command Default

The control plane independent bit setting in outgoing BFD packets is enabled by default.

Command Modes

Global configuration mode (config)

Command History

Release Modification

8.(0)1 This command was introduced.

Usage Guidelines

Enable the BFD feature before using the **bfd c-bit** command.

This example shows how to configure the control plane independent bit setting in outgoing BFD packets:

```
switch# configure terminal
switch(config)# feature bfd
switch(config)# bfd c-bit
switch(config)#
```

This example shows how to disable the control plane independent bit setting in outgoing BFD packets:

```
switch(config)# no bfd c-bit
switch(config)#
```

Related Commands

Command	Description
show running-config bfd	Displays the BFD running configuration.

bfd echo

To enable Bidirectional Forwarding Detection (BFD) echo mode, use the **bfd echo** command. To disable BFD echo mode, use the **no** form of this command.

bfd [{ipv4 | ipv6}] **echo**
no bfd [{ipv4 | ipv6}] **echo**

Syntax Description

ipv4	(Optional) Enables BFD echo mode for the IPv4 address.
ipv6	(Optional) Enables BFD echo mode for the IPv6 address.

Command Default

BFD echo mode is enabled by default.

Command Modes

Interface configuration mode (config-if)

Command History

Release	Modification
6.2(2)	Added ipv4 , ipv6 keywords to the syntax description.
5.0(2)	This command was introduced.

Usage Guidelines

When echo mode is enabled, the required minimum receive interval value is taken from the BFD slow-timer setting.



Note Before using BFD echo mode, you must disable the IP packet verification check for identical IP source and destination addresses by entering the **no hardware ip verify address identical** command in the default virtual device context (VDC).



Note Before using BFD echo mode, you must disable the sending of Internet Control Message Protocol (ICMP) redirect messages by entering the **no ip redirects** command.

Use the **no bfd echo** command to stop sending echo packets and signify that the device is unwilling to forward echo packets that are received from BFD neighbors. The RequiredMinEchoRx BFD session parameter is set to zero when echo mode is disabled.

This command does not require a license.

Examples

This example shows how to configure BFD echo mode:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# bfd ipv4 echo
```

This example shows that the BFD session neighbor is up and using BFD echo mode. The relevant command output is shown in bold in the output:

```
switch# show bfd neighbors details
OurAddr      NeighAddr    LD/RD  RH/RS    Holdown(mult) State   Int
172.16.1.2   172.16.1.1   1/6    Up        0 (3 )   Up     Fa0/1
Session state is UP and using echo function with 50 ms interval.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holdown (hits): 3000(0), Hello (hits): 1000(337)
Rx Count: 341, Rx Interval (ms) min/max/avg: 1/1008/882 last: 364 ms ago
Tx Count: 339, Tx Interval (ms) min/max/avg: 1/1016/886 last: 632 ms ago
Registered protocols: EIGRP
Uptime: 00:05:00
Last packet: Version: 1           - Diagnostic: 0
              State bit: Up       - Demand bit: 0
              Poll bit: 0         - Final bit: 0
              Multiplier: 3       - Length: 24
              My Discr.: 6        - Your Discr.: 1
              Min tx interval: 1000000 - Min rx interval: 1000000
              Min Echo interval: 50000
```

Related Commands

Command	Description
bfd interval	Configures the BFD session parameters.
bfd slow-timer	Configures the BFD RequiredminEchoRx interval.
feature bfd	Enables the BFD feature.
hardware ip verify address identical	Enables the verification of IP packets do not have the same address for IP source and IP destination fields.
ip redirects	Enables the sending of ICMP redirect messages if the Cisco IOS software is forced to resend a packet through the same interface on which it was received.

bfd interval

To configure the Bidirectional Forwarding Detection (BFD) session parameters, use the **bfd interval** command. To return to the default setting, use the **no** form of this command.

bfd [{ipv4 | ipv6}] **interval** *mintx* *min_rx* *msec* **multiplier** *value*
no **bfd** [{ipv4 | ipv6}] **interval** *mintx* *min_rx* *msec* **multiplier** *value*

Syntax Description

ipv4	(Optional) Configures BFD session parameters for the IPv4 address.
ipv6	(Optional) Configures BFD session parameters for the IPv6 address.
<i>mintx</i>	Rate at which BFD control packets are sent to BFD neighbors. The configurable range is from 50 to 999.
min_rx <i>msec</i>	Specifies the rate at which BFD control packets are expected to be received from BFD neighbors. The range is from 50 to 999.
multiplier <i>value</i>	Specifies the number of consecutive BFD control packets that must be missed from a BFD neighbor before BFD declares that the neighbor is unavailable and the BFD neighbor is informed of the failure. The range is from 1 to 50.

Command Default

BFD interval: 50 milliseconds

min_rx: 50 milliseconds

multiplier: 3

Command Modes

Global configuration mode

Interface configuration mode

Command History

Release	Modification
6.2(2)	Added ipv4, ipv6 keywords to the syntax description.
5.0(2)	This command was introduced.

Usage Guidelines

BFD session parameters configured at the interface level take precedence over the globally configured BFD session parameters.

This command does not require a license.

Examples

This example shows how to set the BFD session parameters for Ethernet interface 3/1:

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# bfd ipv6 interval 50 min_rx 20 multiplier 3
```

Related Commands

Command	Description
feature bfd	Enables the BFD feature.
show bfd neighbors	Displays information about BFD neighbors.

bfd multihop authentication

To configure SHA-1 authentication for all Bidirectional Forwarding Detection (BFD) multihop sessions for the BGP neighbor, use the **bfd multihop authentication** command. To remove the SHA-1 authentication configuration, use the **no** form of this command.

```
bfd multihop authentication keyed-SHA1 key-id id {hex-key | key ascii-key}
no bfd multihop authentication keyed-SHA1 key-id id {hex-key | key ascii-key}
```

Syntax Description

key-id	Specifies the key ID to use in BFD frames.
<i>id</i>	Key ID value. The range is from 1 to 255.
<i>hex-key</i>	HEX binary SHA1 secret. A hex-key can be any case-sensitive, alphanumeric string up to 40 characters.
key	Specifies the ASCII SHA1 secret.
<i>ascii-key</i>	SHA1 secret value. An ASCII key can be any case-sensitive, alphanumeric string up to 20 characters.

Command Default

None

Command Modes

Neighbor configuration mode (config-router-neighbor)

Command History

Release	Modification
8.1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure BFD multihop session on BGP:

```
switch# configure terminal
switch(config)#router bgp 200
switch(config-if)# neighbor 10.1.1.2 remote-as 200
switch(config-router)# bfd
switch(config-router-neighbor)# bfd multihop interval 250 min_rx 250 multiplier 10
switch(config-router-neighbor)# bfd multihop authentication keyed-SHA1 keyid 20 key sha
```

Related Commands

Command	Description
show running-config bfd	Displays the BFD running configuration.
show running-config interface	Displays the running configuration for a specific interface.

bfd multihop hosting-linecard

To configure the hosting linecard for the Bidirectional Forwarding Detection (BFD) multihop sessions, use the **bfd multihop hosting-linecard** command.

bfd multihop hosting-linecard add module *module-number*

Syntax Description	<i>module-number</i>	Specifies the module number.
---------------------------	----------------------	------------------------------

Command Default	None
------------------------	------

Command Modes	Global configuration mode
----------------------	---------------------------

Command History	Release	Modification
	8.1(1)	This command was introduced.

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples	This example shows how to add a hosting linecard for the BFD multihop sessions:
-----------------	---

```
switch# configure terminal
switch(config)# bfd multihop hosting-linecard add module 10
switch(config)# end
```

Related Commands	Command	Description
	feature bfd	Enables the BFD feature.
	show bfd neighbors	Displays information about BFD neighbors.

bfd multihop interval

To configure the Bidirectional Forwarding Detection (BFD) multihop session parameters, use the **bfd multihop interval** command. To return to the default setting, use the **no** form of this command.

bfd multihop interval *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier*

no bfd multihop interval *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier*

Syntax Description

<i>milliseconds</i>	Rate at which BFD control packets are sent to BFD neighbors. The configurable range is from 250 to 999 milliseconds.
min_rx	Specifies the rate at which BFD control packets are expected to be received from BFD neighbors.
<i>interval-multiplier</i>	Specifies the number of consecutive BFD control packets that must be missed from a BFD neighbor before BFD declares that the neighbor is unavailable and the BFD neighbor is informed of the failure. The range is from 3 to 250.

Command Default

BFD interval: 250 milliseconds

min_rx: 250 milliseconds

multiplier: 3

Command Modes

Global configuration mode

Neighbor configuration mode

Command History

Release	Modification
8.1(1)	This command was introduced.

Usage Guidelines

The interval value configured for the BGP neighbor is used for the BFD multihop session. If the interval value is not configured for the BGP neighbor, the value configured by using the **bfd multihop interval** command is considered. If the interval values are not configured in any case, then the default values are used.

This command does not require a license.

Examples

This example shows how to set the BFD multihop session parameters:

```
switch# configure terminal
switch(config)# bfd multihop interval 250 min_rx 250 multiplier 10
switch(config)# end
```

This example shows how to set the BFD multihop session parameters for BFD neighbor:

```
switch# configure terminal
switch(config)# neighbor 10.1.1.2 remote-as 200
switch(config-router)# bfd
switch(config-router-neighbor)# bfd multihop interval 250 min_rx 250 multiplier 10
```

Related Commands

Command	Description
feature bfd	Enables the BFD feature.
show bfd neighbors	Displays information about BFD neighbors.

bfd optimize subinterfaces

To optimize subinterfaces on a physical interface for Bidirectional Forwarding Detection (BFD), use the **bfd optimize subinterfaces** command. To return to the default setting, use the **no** form of this command.

bfd optimize subinterfaces
no bfd optimize subinterfaces

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Interface configuration mode

Command History	Release	Modification
	5.0(2)	This command was introduced.

Usage Guidelines You can optimize subinterfaces, because BFD creates sessions for all configured subinterfaces. BFD sets the subinterface with the lowest configured VLAN ID as the master subinterface and that subinterface uses the BFD session parameters of the parent interface. The remaining subinterfaces use the slow timer. If the master subinterface session detects an error, BFD marks all subinterfaces on that physical interface as down.

When the lowest configured VLAN has both an IPv4 and an IPv6 BFD session, there is no deterministic way to say which of the two sessions is always chosen as the master session.

This command does not require a license.

Examples This example shows how to enable subinterface optimization:

```
switch(config)# interface Ethernet 1/1
switch(config-if)# bfd
optimize subinterfaces
```

Related Commands	Command	Description
	feature bfd	Enables the BFD feature.

bfd per-link

To enable Bidirectional Forwarding Detection (BFD) for all links in a port channel, use the **bfd per-link** command. To disable BFD for a port channel, use the **no** form of this command.

bfd per-link
no bfd per-link

Syntax Description

This command has no arguments or keywords.

Command Default

BFD is not enabled on the port channel.

Command Modes

Port channel configuration mode

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

Use the **bfd per-link** command to enable BFD on each link in a port channel. BFD creates a session for each link in the port channel and provides an aggregate result to client protocols. For example, if the BFD session for one link on a port channel is up, BFD informs client protocols such as Open Shortest Path First (OSPF) that the port channel is up. The BFD session parameters are negotiated between the BFD peers in a three-way handshake.

bfd Per-link is not allowed with echo mode, or when there are BFD sessions on the port-channel. The port-channel must be shutdown before configuring per-link.

This command does not require a license.

Examples

This example shows how to enable BFD for port channel 3:

```
switch# configure terminal
switch(config)# interface port-channel 3
switch(config)# shutdown
switch(config-if)# bfd per-link
```

This example shows how to configure the BFD session parameters for a port channel:

```
switch# configure terminal
switch(config)# interface port-channel 3
switch(config-if)# bfd interval 50 min_rx 50 multiplier 3
```

Related Commands

Command	Description
bfd echo	Enables BFD echo mode.
bfd interval	Configures the BFD session parameters

Command	Description
feature bfd	Enables the BFD feature.

bfd slow-timer

To configure the Bidirectional Forwarding Detection (BFD) slow timer value, use the **bfd slow-timer** command. To return to the default setting, use the **no** form of this command.

```
bfd [{ipv4 | ipv6}] slow-timer milliseconds
no [{ipv4 | ipv6}] bfd slow-timer milliseconds
```

Syntax Description	Field	Description
	ipv4	Configures the slow timer in milliseconds, used in the echo function for the IPv4 address.
	ipv6	Configures the slow timer in milliseconds, used in the echo function for the IPv6 address.
	<i>milliseconds</i>	BFD slow timer value, in milliseconds. The range is from 1000 to 30000.

Command Default The default BFD slow timer value is 2000 milliseconds.

Command Modes Global configuration mode
Interface configuration mode

Command History	Release	Modification
	6.2(2)	Added ipv4, ipv6 keywords to the syntax description.
	5.0(2)	This command was introduced.

Usage Guidelines Use the **bfd slow-timer** command to configure how fast a BFD session comes up. This value also sets the RequiredMinRx (or min_rx) value when echo mode is enabled.

This command does not require a license.

Examples This example shows that the BFD slow timer value is configured to 14,000 milliseconds for IPv6:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# bfd ipv6 slow-timer 14000
switch(config-if)#
```

This example shows that the BFD slow timer value of 14,000 milliseconds has been implemented. The values for the MinTxInt and MinRxInt correspond to the configured value for the BFD slow timer. The relevant command output is shown in bold.

```
switch# show bfd neighbors details
OurAddr      NeighAddr    LD/RD  RH/RS  Holdown(mult)  State  Int
172.16.10.1  172.16.10.2  1/1    Up      0 (3)          Up     Et2/0
Session state is UP and using echo function with 50 ms interval.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 14000, MinRxInt: 14000
, Multiplier: 3
Received MinRxInt: 10000, Received Multiplier: 3
Holdown (hits): 3600(0), Hello (hits): 1200(418)
Rx Count: 422, Rx Interval (ms) min/max/avg: 1/1480/1087 last: 112 ms ago
Tx Count: 420, Tx Interval (ms) min/max/avg: 1/2088/1090 last: 872 ms ago
```

```
Registered protocols: OSPF
Uptime: 00:07:37
Last packet: Version: 1           - Diagnostic: 0
              State bit: Up       - Demand bit: 0
              Poll bit: 0         - Final bit: 0
              Multiplier: 3       - Length: 24
              My Discr.: 1        - Your Discr.: 1
              Min tx interval: 14000 - Min rx interval: 14000
              Min Echo interval: 4000
```

Related Commands

Command	Description
bfd echo	Enables BFD echo mode.



C Commands

- [capabilities-conflict](#), on page 26
- [carrier-delay](#), on page 28
- [channel-group](#), on page 30
- [clear counters interface](#), on page 34
- [clear l2protocol tunnel counters](#), on page 36
- [clear lacp counters](#), on page 37
- [clear vpc statistics](#), on page 38
- [config-sync](#), on page 39
- [connection timeout](#), on page 40
- [critical-event](#), on page 42

capabilities-conflict

To configure what action is taken on an interface when a capabilities-conflict event occurs, use the **capabilities-conflict** command in Ethernet OAM action configuration mode or interface Ethernet OAM action configuration mode. To remove the configuration, use the **no** form of this command.

capabilities-conflict {**disable** | **efd** | **error-disable-interface** | **log**}

no capabilities-conflict {**disable** | **efd** | **error-disable-interface** | **log**}

Syntax Description	Option	Description
	disable	Performs no action on the interface when a capabilities-conflict event occurs.
	efd	Puts the line protocol into the down state for an interface when a capabilities-conflict event occurs. The state is removed when the first packet is received without a conflict.
	error-disable-interface	Puts the interface into the error-disable state when a capabilities-conflict event occurs.
	log	(Interface Ethernet OAM action configuration only) Creates a syslog entry when a capabilities-conflict event occurs. This action is available in Interface Ethernet OAM action configuration mode to override the profile setting and log the event for the interface when it occurs.

Command Default The default action is to create a syslog entry.

Command Modes Ethernet OAM action configuration (config-eoam-action)
Interface Ethernet OAM action configuration (config-if-eoam-action)

Supported User Roles

network-admin

vdc---admin

network---operator

vdc-operator

Command History	Release	Modification
	7.3(0)D1(1)	This command was introduced.

Usage Guidelines This command does not require a license.

The following example shows how to configure that no action is performed on the interface when a critical-event notification is received:

```
switch# configure terminal
switch(config)# ethernet oam profile Profile_1
switch(config-eoam)# action
switch(config-eoam-action)# critical-event disable
```

The following example shows how to configure that the interface is put into the error-disable state when a critical-event notification is received:

```
switch# configure terminal
switch(config)# ethernet oam profile Profile_1
switch(config-eoam)# action
switch(config-eoam-action)# critical-event error-disable-interface
```

The following example shows how to configure that a syslog is created when a critical-event notification is received:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ethernet oam
switch(config-if-eoam)# action
switch(config-if-eoam-action)# critical-event log
```

Related Commands

Command	Description
ethernet oam profile	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam	Attaches an Ethernet OAM profile to an interface.
profile (EOAM)	Attaches an Ethernet OAM profile to an interface.

carrier-delay

To set the carrier delay on an interface, use the **carrier-delay** command. To return to the default carrier delay value, use the **no** form of this command.

carrier-delay {*sec* | **msec** *value*}

no carrier-delay

Syntax Description

<i>sec</i>	Seconds of delay. The range is from 0 to 60.
msec	Specifies milliseconds of delay.
<i>value</i>	Milliseconds of delay. The range is from 0 to 1000.

Command Default

The default is 100 milliseconds.

Command Modes

Interface VLAN configuration mode

network-admin

vdc-admin

Command History

Release	Modification
4.0(3)	This command was introduced.

Usage Guidelines



Note You must enable the VLAN interface feature, using the **feature interface-vlan** command, before you can use this command.

If a link goes down and comes back up before the carrier delay timer expires, the down state is effectively filtered, and the rest of the software on the device is not aware that a link-down event occurred. A large carrier delay timer results in fewer link-up/link-down events being detected. When you set the carrier delay time to 0, the device detects each link-up/link-down event that occurs.



Note The **carrier-delay** command is supported only on the VLAN interface mode; no other interface modes support this command.

In most environments, a lower carrier delay time is better than a higher one. The value that you choose depends on the nature of the link outages and how long you expect these linkages to last in your network. If your data links are subject to short outages (especially if those outages last less time than it takes for your IP routing to converge), you should set a long carrier delay value to prevent these short outages from causing unnecessary

churn in your routing tables. However, if you outages tend to be longer, then you may want to set a shorter carrier delay time so that the outages are detected sooner, and the IP route convergence begins and ends sooner.

This command does not require a license.

Examples

This example shows how to set the carrier delay timer to 20 minutes for VLAN 6:

```
switch(config)#  
interface vlan  
6  
switch(config-if)#  
carrier-delay 20  
switch(config-if)#
```

Related Commands

Command	Description
show interface vlan	Displays information about VLAN interfaces.

channel-group

To assign and configure a physical interface to a port-channel group, use the **channel-group** command. To remove the channel-group configuration from the interface, use the **no** form of this command.

channel-group *number* [**force**] [**mode** {**active** | **on** | **passive**}]

no channel-group [*number*]

Syntax Description

number	Number of the channel group. The maximum number of port channels that can be configured is 256 across all virtual device contexts (VDCs), and the range is from 1 to 4096.
force	(Optional) Forces the interface to join the channel group, although some parameters are not compatible. For information on the compatibility parameters and which ones can be forced, see the Usage Guidelines section.
mode	Specifies the port-channel mode of the interface.
active	Specifies that when you enable the Link Aggregation Control Protocol (LACP), this command enables LACP on the specified interface. The interface is in an active negotiating state, in which the port initiates negotiations with other ports by sending LACP packets.
on	Specifies the default channel mode and all port channels that are not running LACP remain in this mode. If you attempt to change the channel mode to active or passive before enabling LACP, the device returns an error message. After you enable LACP globally by using the feature lacp command, you enable LACP on each channel by configuring the channel mode as either active or passive. An interface in this mode does not initiate or respond to LACP packets. When an LACP attempts to negotiate with an interface in the on state, it does not receive any LACP packets and becomes an individual link with that interface; it does not join the channel group. The default mode is on .
passive	Specifies that when you enable LACP, this command enables LACP only if an LACP device is detected. The interface is in a passive negotiation state, in which the port responds to LACP packets that it receives but does not initiate LACP negotiation.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use this command to create a channel group that includes the interface that you are working on and to add or remove specific interfaces from the channel group. Use this command to move a port from one channel group to another. You enter the channel group that you want the port to move to; the device automatically removes the specified port from its present channel group and adds that port to the specified channel group.

After you enable LACP globally by using the feature `lacp` command, you enable LACP on each channel by configuring the channel mode as either **active** or **passive**. A port channel in the **on** channel mode is a pure port channel and can aggregate a maximum of eight ports. It does not run LACP.

You cannot change the mode for an existing port channel or any of its interfaces if that port channel is not running LACP; the channel mode remains as **on**. The system returns an error message if you try.

All ports in one port channel must be in the same virtual device context (VDC). With LACP enabled, this requirement applies to the possible eight active ports and the possible eight standby ports. The port channels can originate in one VDC (with all ports in that channel in the same VDC) and partner with a port channel in another VDC (again, all ports in that channel must be in that VDC).

Use the **no** form of this command to remove the physical interface from the port channel. When you delete the last physical interface from a port channel, the port channel remains. To delete the port channel completely, use the **no form of this interface port-channel** command.

The compatibility check includes the following operational attributes:

- Network layer
- (Link) speed capability
- Speed configuration
- Duplex capability
- Duplex configuration
- Port mode
- Access VLAN
- Trunk native VLAN
- Tagged or untagged
- Allowed VLAN list
- MTU size
- SPAN—Cannot be a SPAN source or destination port
- Layer 3 Ports—Cannot have subinterfaces
- Storm control
- Flow control capability
- Flow control configuration

Use the **show port-channel compatibility-parameters** command to see the full list of compatibility checks that the Cisco NX-OS uses.

You can only add interfaces configured with the channel mode set to **on** to static port channels, that is without a configured aggregation protocol and you can only add interfaces configured with the channel mode as **active** or **passive** to port channels that are running LACP.

You can configure these attributes on an individual member port. If you configure a member port with an incompatible attribute, Cisco NX-OS suspends that port in the port channel.

Alternatively, you can force ports with incompatible parameters to join the port channel as long the following parameters are the same:

- (Link) speed capability
- Speed configuration
- Duplex capability
- Duplex configuration
- Flow control capability
- Flow control configuration

When the interface joins a port channel, some of its individual parameters are removed and replaced with the values on the port channel as follows:

- Bandwidth
- Delay
- Extended Authentication Protocol over UDP
- VRF
- IP address (v4 and v6)
- MAC address
- Spanning Tree Protocol
- NAC
- Service policy
- Quality of Service (QoS)
- ACLs

Many of the following interface parameters remain unaffected when the interface joins or leaves a port channel:

- Beacon
- Description
- CDP
- LACP port priority
- Debounce
- UDLD
- MDIX
- Rate mode
- Shutdown
- SNMP trap

If subinterfaces are configured for the port-channel interface and a member port is removed from the port channel, the configuration of the port-channel subinterface is not propagated to the member ports.

Any configuration changes that you make in any of the compatibility parameters 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).

You do not have to create a port-channel interface before you assign 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 can create either a Layer 2 or a Layer 3 port channel 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 or dynamically.



Note The number of ports allowed in a port channel (for the ON mode) is different between M1 Series modules and F1 Series modules on VDCs only. The number is 8 for M1 Series modules or M1-F1 Series VDCs and 16 for F1 Series modules.

This command does not require a license.

Examples

This example shows how to add an interface to LACP channel group 5 in active mode:

```
switch(config-if)# channel-group 5 mode active
switch(config-if)#
```

Related Commands

Command	Description
show interface port-channel	Displays information about the traffic on the specified port-channel interface.
show lacp	Displays LACP information.
show port-channel summary	Displays information about the port channels.

clear counters interface

To clear the Ethernet and management interface counters, use the **clear counters interface** command.

clear counters interface {**all**[snmp] | **ethernet**slot/port | **loopback**number | **mgmt**number | **port-channel**channel-number | **tunnel**tunnel-number | **vlan**vlan-number}

Syntax Description

all	Clears all interface counters.
snmp	(Optional) clears SNMP interface counters.
ethernet slot/port	Clears the Ethernet interface counter for the slot number and port number specified.
loopback number	Clears the loopback interface counter for the virtual interface number specified. The range is from 0 to 1023.
mgmt number	Clears the management interface counter for the number specified. The number is 0.
port-channel channel-number	Clears the port-channel interface for the number specified. The range is from 1 to 4096.
tunnel tunnel-number	Clears the port-channel interface for the number specified. The range is from 0 to 65535.
vlan vlan-number	Clears the port-channel interface for the number specified. The range is from 1 to 4096.

Command Default

None

Command Modes

Global configuration mode

Interface Configuration mode

Command History

Release	Modification
6.2(2)	Added the snmp keyword to the syntax description.
4.0	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to clear an SNMP counter interface:

```
switch# clear counters interface all snmp
```

This example shows how to clear and reset the counters on Ethernet port 5/5:

```
switch# clear counters interface ethernet 5/5
```

Related Commands

Command	Description
show interface counters	Displays in and out counters for all interfaces in the system.

clear l2protocol tunnel counters

To clear the Layer 2 protocol tunnel statistics counters, use the **clear l2protocol tunnel counters** command.

clear l2protocol tunnel counters [**interface** *if-range*]

Syntax Description	interface	(Optional) Specifies the interface statistics to clear.
	<i>if-range</i>	Range of interfaces.

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	5.0(2)	This command was introduced.

Usage Guidelines If no interfaces are specified, the Layer 2 protocol tunnel statistics are cleared for all interfaces.

This command does not require a license.

Examples

This example shows how to clear the Layer 2 protocol tunnel statistics counters:

```
switch# clear
      l2protocol tunnel
counters
```

Related Commands	Command	Description
	show l2protocol tunnel	Displays Layer 2 protocol tunnel information.

clear lacp counters

To clear the statistics for all interfaces for Link Aggregation Control Protocol (LACP) groups, use the **clear lacp counters** command.

clear lacp counters [**interface port-channel** *channel-number*]

Syntax Description	interface port-channel	(Optional) Specifies the interface port channel.
	<i>channel-number</i>	(Optional) LACP port-channel number. The range is from 1 to 4096.

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	4.0	This command was introduced.

Usage Guidelines If you enter this command for a static port-channel group without enabling the aggregation protocol, the device ignores the command.

If you do not specify a channel number, the LACP counters for all LACP port groups are cleared.

This command does not require a license.

Examples

This example shows how to clear all LACP counters:

```
switch(config)# clear lacp counters
switch(config)#
```

This example shows how to clear all LACP counters for the LACP port-channel group 20:

```
switch(config)# clear lacp counters interface port-channel 20
switch(config)#
```

Related Commands	Command	Description
	show lacp counters	Displays information about LACP statistics.

clear vpc statistics

To clear virtual port-channel (vPC) statistics, use the **clear vpc statistics** command.

clear vpc statistics {**all** | **peer-keepalive** | **peer-link** | **vpc number**}

Syntax Description		
	all	Clears all vPC statistics on the local vPC peer device.
	peer-keepalive	Clears the vPC peer-keepalive statistics on the local vPC peer device.
	peer-link	Clears statistics on the local vPC peer device.
	vpc number	Clears vPC statistics on the specified vPC. The range is from 1 to 4096.

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	4.1(3)	This command was introduced.

Usage Guidelines Use the **clear vpc statistics** command to clear the vPC statistics. If the feature is not enabled, this command is unavailable.

The **clear vpc statistics peer-link** and **clear vpc statistics vpc number** commands are redirected to the appropriate port channel and the **clear statistics port-channel channel-number** command.

This command does not require a license.

Examples

This example shows how to clear the statistics for vPC 10:

```
switch(config)# clear vpc statistics vpc 10
switch(config) #
```

Related Commands	Command	Description
	show vpc statistics	Displays vPC statistical information on vPCs. If the feature is not enabled, the system displays an error when you enter this command.

config-sync

To enable virtual port channels (vPC) configuration synchronization, use the **config-sync** command. To disable vPC configuration synchronization, use the **no** form of this command.

config-sync
no config-sync

Syntax Description This command has no arguments or keywords.

Command Default Disabled.

Command Modes VPC domain configuration mode

Release	Modification
7.1(1)D1(0)	This command was introduced.

Usage Guidelines You must configure this command on both the primary and secondary switches in the same vPC domain. It does not matter which switch you configure first.

The **config-sync** command enables the synchronization of the configuration between the two switches. The following types of commands are enabled for configuration synchronization:

- Type-1 configurations:
 - Global configurations
 - vPC member port-channel configurations
- Type-2 configurations:
 - Global configurations
- vPC configurations.

This command does not require a license.

Examples

This example shows how to enable configuration synchronization for switch 1 and switch 2:

```
n7k-1# configure terminal
n7k-1 (config)# vpc domain 300
n7k-1 (config-vpc-domain)# config-sync
n7k-2# configure terminal
n7k-2 (config)# vpc domain 300
n7k-2 (config-vpc-domain)# config-sync
```

Related Commands

Command	Description
showvpc config-sync database	Displays list of commands that are enabled with configuration synchronization .

connection timeout

To configure the timeout value for an Ethernet OAM session, use the **connection timeout** command in Ethernet OAM configuration mode. To remove the configuration, use the **no** form of this command.

connection timeout *seconds*
no connection timeout [*seconds*]

Syntax Description	<i>seconds</i> Connection timeout period in number of lost periodic information OAMPDUs. The range is 2 to 30. The default value is 5.
---------------------------	--

Command Default	None
------------------------	------

Command Modes	Ethernet OAM action configuration (config-eoam-action) Interface Ethernet OAM action configuration (config-if-eoam-action)
----------------------	---

Supported User Roles

network-admin
vdc--admin
network---operator
vdc-operator

Command History	Release	Modification
	7.3(0)D1(1)	This command was introduced.

Usage Guidelines	If no packets are received from the OAM peer in the specified connection timeout period which is measured in number of lost periodic Information OAMPDUs, then the OAM session is brought down, and the negotiation phase starts again.
-------------------------	---

This command does not require a license.

This example shows how to configure the connection timeout value of an Ethernet OAM session:

```
switch# configure terminal
switch(config)# ethernet oam profile Profile_1
switch(config-eoam)# connection timeout 20
```

Related Commands	Command	Description
	action discovery-timeout	Configures what action is taken on an interface when a connection timeout occurs.
	ethernet oam	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
	ethernet oam profile	Creates an EOAM profile and enters EOAM configuration mode.

Command	Description
show ethernet oam configuration	Displays the current active Ethernet OAM configuration on an interface.
show ethernet oam discovery	Displays the current status of Ethernet OAM sessions.
show ethernet oam interfaces	Displays the current state of Ethernet OAM interfaces.

critical-event

To configure what action is taken on an interface when a critical-event notification is received from the remote Ethernet OAM peer, use the **critical-event** command in Ethernet OAM action configuration action mode or interface Ethernet OAM action configuration mode. To remove the configuration, use the **no** form of this command.

```
critical-event {disable | error-disable-interface | log}
no critical-event [{disable | error-disable-interface | log}]
```

Syntax Description	disable	error-disable-interface	log
	Performs no action on the interface when a critical-event notification is received.	Puts the interface into the error-disable state when a critical-event notification is received.	(Interface Ethernet OAM action configuration only) Creates a syslog entry when a critical-event notification is received. This action is available in Interface Ethernet OAM action configuration mode to override the profile setting and log the event for the interface when it occurs.

Command Default The default action is to create a syslog entry.

Command Modes Ethernet OAM action configuration (config-eoam-action)
Interface Ethernet OAM action configuration (config-if-eoam-action)

Supported User Roles

```
network-admin
vdc--admin
network--operator
vdc-operator
```

Command History	Release	Modification
	7.3(0)D1(1)	This command was introduced.

Usage Guidelines This command does not require a license.

The following example shows how to configure that no action is performed on the interface when a critical-event notification is received:

```
switch# configure terminal
switch(config)# ethernet oam profile Profile_1
switch(config-eoam)# action
switch(config-eoam-action)# critical-event disable
```

The following example shows how to configure that the interface is put into the error-disable state when a critical-event notification is received:

```
switch# configure terminal
switch(config)# ethernet oam profile Profile_1
switch(config-eoam)# action
switch(config-eoam-action)# critical-event error-disable-interface
```

The following example shows how to configure that a syslog is created when a critical-event notification is received:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ethernet oam
switch(config-if-eoam)# action
switch(config-if-eoam-action)# critical-event log
```

Related Commands

Command	Description
ethernet oam profile	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam	Attaches an Ethernet OAM profile to an interface.
profile (EOAM)	



D Commands

- [default interface](#), on page 46
- [delay](#), on page 47
- [delay restore](#), on page 48
- [delay restore interface-vlan](#), on page 49
- [delay restore interface-vlan batch](#), on page 50
- [description](#), on page 51
- [discovery-timeout](#), on page 52
- [dual-active exclude interface-vlan](#), on page 54
- [duplex](#), on page 55
- [dying-gasp](#), on page 56

default interface

To create a checkpoint of the running configuration for rollback purposes, use the **default interface** command.

default interface *if* [**checkpoint** *name*]

Syntax Description		
	<i>if</i>	Interface type and number in module/slot format.
	checkpoint	(Optional) Creates a configuration rollback checkpoint.
	<i>name</i>	(Optional) Checkpoint name. The maximum size is 80 alphanumeric characters.

Command Default None

Command Modes Interface configuration mode

Command History	Release	Modification
	5.1(1)	This command was introduced.

Usage Guidelines Use this command to return an interface to its default state. All the user configuration under the specified interface(s) is deleted upon the successful completion of the command. You can optionally create a checkpoint before deleting the interface configuration, so that you can later choose to roll back to the original configuration.



Caution

When using this command, you delete the configuration of the specified interfaces unless you enter the checkpoint keyword. The optional checkpoint keyword allows you to create a checkpoint of the interface configuration to that you can later roll back to the original configuration.

This command does not require a license.

Examples

This example shows how to create a checkpoint of the running configuration for rollback purposes:

```
switch(config)# default interface ethernet 2/1 checkpoint test
.....Done
switch(config)#
```

Related Commands	Command	Description
	show interface switchport	Displays the administrative and operational status of a switching (nonrouting) port.

delay

To configure the interface throughput delay for Ethernet interfaces, use the **delay** command. To remove the configured throughput delay, use the **no** form of this command.

delay *value*
no delay

Syntax Description

<i>value</i>	Delay time in tens of microseconds. The range is from 1 to 16777215.
--------------	--

Command Default

10 microseconds for all interfaces except loopback ports
 5000 microseconds for loopback ports

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Beginning with Cisco NX-OS Release 4.2(1) for the Cisco Nexus 7000 Series devices, the default delay values are changed. Prior to this release, all the default delay value for all interfaces was 100 microseconds.

After upgrading from an older release, when you enter the **show running** command on a VLAN interface, the display shows an additional configuration of “delay 100.” If you want to revert the delay value to the new default, enter the **no delay** command for that VLAN interface.

Specifying a value for the throughput delay provides a value for use by Layer 3 protocols; it does not change the actual throughput delay of an interface.

This command does not require a license.

Examples

This example shows how to configure the throughput-delay time to 100,000 microseconds for the slot 3 port 1 Ethernet interface:

```
switch(config)# interface ethernet 3/1
switch(config-if)# delay 10000
```

Related Commands

Command	Description
show interface	Displays information about the interface, which includes the delay parameter.

delay restore

To delay the virtual port channel (vPC) from coming up on the restored vPC peer device after a reload when the peer adjacency is already established, use the **delay restore** command. To return to the default value, use the **no** form of this command.

delay restore *seconds*
no delay restore *seconds*

Syntax Description	<i>seconds</i> Number of seconds to delay bringing up the restored vPC peer device. The range is from 1 to 3600.
---------------------------	--

Command Default 30 seconds

Command Modes vpc-domain command mode

Command History	Release	Modification
	4.2(1)	This command was introduced.

Usage Guidelines Use the delay restore command to avoid upstream traffic from the access device to the core from being dropped when you restore the vPC peer devices. If the restored vPCs come up before the routing tables are converged, you might see packet drops.

This command does not require a license.

Examples

This example shows how to configure the delay reload:

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# delay restore 40
```

Related Commands	Command	Description
	delay restore interface-vlan	Allows Layer 3 routing protocols to converge and Forwarding Information Base (FIB) programming to complete for a more graceful restoration of switched virtual interfaces (SVIs).
	feature vpc	Enables vPC configuration on the device.

delay restore interface-vlan

To allow Layer 3 routing protocols to converge and Forwarding Information Base (FIB) programming to complete for a more graceful restoration of switched virtual interfaces (SVIs) on the restored virtual port channel (vPC) after the delay of the vPC from coming up on the restored vPC peer device, use the **delay restore interface-vlan** command. To return to the default value, use the **no** form of this command.

delay restore interface-vlan *seconds*
no delay restore interface-vlan *seconds*

Syntax Description	<i>seconds</i> Number of seconds to delay bringing up the SVIs on the vPC peer device. The range is from 1 to 3600.
---------------------------	---

Command Default 10 seconds

Command Modes vpc-domain command mode

Command History	Release	Modification
	4.2(1)	This command was introduced.

Usage Guidelines Use the delay restore command to avoid upstream traffic from the access device to the core from being dropped when you restore the vPC peer devices. If the restored vPCs come up before the routing tables are converged, you might see packet drops.

This command does not require a license.

Examples

This example shows how to configure the delay reload:

```
switch# configure terminal
switch(config)# vpc domain 1
switch(config-vpc-domain)# delay restore 60
switch(config-vpc-domain)# delay restore interface-vlan 30
switch(config-vpc-domain)#
```

Related Commands	Command	Description
	delay restore	Delays the virtual port channel (vPC) from coming up on the restored vPC peer device after a reload when the peer adjacency is already established.
	feature vpc	Enables vPC configuration on the device.

delay restore interface-vlan batch

This command is used to configure the batching to bring up the interface-vlan or bridge-domain interfaces on vPC secondary.

To return to the default value, use the **no** form of this command.

delay restore interface-vlan batch *batch size* **timer** *time in seconds*
no delay restore interface-vlan batch *batch size* **timer** *time in seconds*

Syntax Description

Table 1: Syntax Description

<i>Batch size</i>	Number of interface-vlan or interface-bridge-domain brought up per batch. The range is from 1 to 4094.
<i>seconds</i>	Number of seconds to delay in bringing up the next batch of interface-vlan or interface-bridge-domain. The range is from 1 to 3600.

Command Modes

vpc-domain command mode

Command Default

vPC delay restore <time-out>

Release	Modification
8.2(7)	This command was introduced.

Examples

This example shows how to enable batching of SVIs on VPC secondary upon expiry of the delay restore interface-vlan timer:

```
switch(config)# vpc domain 1
switch(config-vpc-domain)# delay restore
switch(config-vpc-domain)# delay restore interface-vlan
switch(config-vpc-domain)# delay restore interface-vlan batch 200
switch(config-vpc-domain)# delay restore interface-vlan batch 200 timer 20
```

description

To provide textual interface descriptions for the Ethernet and management interfaces, use the **description** command. To remove the description, use the **no** form of this command.

description *text*

Syntax Description

<i>text</i>	Description for the interface that you are configuring. The maximum range is 80 alphanumeric, case-sensitive characters.
-------------	--

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

You use the description command to provide textual interface descriptions.

This command does not require a license.

Examples

This example shows how to add the description server1 to the Ethernet interface on slot 5, port 2:

```
switch(config)# interface ethernet 5/1
switch(config-if)# description server1
```

Related Commands

Command	Description
show interface	Displays information about the interface, which includes the description parameter.

discovery-timeout

To configure what action is taken on an interface when a connection timeout occurs, use the **discovery-timeout** command in Ethernet OAM action configuration mode or interface Ethernet OAM action configuration mode. To remove the configuration, use the **no** form of this command.

discovery-timeout {**disable** | **efd** | **error-disable-interface** | **log**}
nodiscovery-timeout {**disable** | **efd** | **error-disable-interface** | **log**}

Syntax Description	Parameter	Description
	disable	Performs no action on the interface when a connection timeout occurs.
	efd	Puts the line protocol into the down state for an interface when a connection timeout occurs. The state is removed when the session is re-established.
	error-disable-interface	Puts the interface into the error-disable state when a connection timeout occurs.
	log	(Interface Ethernet OAM action configuration only) Creates a syslog entry when a capabilities-conflict event occurs. This action is available in Interface Ethernet OAM action configuration mode to override the profile setting and log the event for the interface when it occurs.

Command Default The default action is to create a syslog entry.

Command Modes Ethernet OAM action configuration (config-eoam-action)
 Interface Ethernet OAM action configuration (config-if-eoam-action)

Command History	Release	Modification
	7.3(0)D1(1)	This command was introduced.

Usage Guidelines This command does not require a license.

The following example shows how to configure that no action is performed on the interface when a connection timeout occurs:

```
switch# configure terminal
switch(config)# ethernet oam profile Profile_1
switch(config-eoam)# action
switch(config-eoam-action)# discovery-timeout disable
```

The following example shows how to configure putting the interface into the line-protocol-down state when a connection timeout occurs.

```
switch# configure terminal
switch(config)# ethernet oam profile Profile_1
switch(config-eoam)# action
switch(config-eoam-action)# discovery-timeout efd
```

The following example shows how to configure that the interface is put into the error-disable state when a connection timeout occurs:

```
switch# configure terminal
switch(config)# ethernet oam profile Profile_1
```

```
switch(config-eoam) # action
switch(config-eoam-action) # discovery-timeout error-disable-interface
```

The following example shows how to configure that a syslog is created when a connection timeout occurs:

```
switch# configure terminal
switch(config) # interface ethernet 2/1
switch(config-if) # ethernet oam
switch(config-if-eoam) # action
switch(config-if-eoam-action) # connection-timeout log
```

Related Commands

Command	Description
ethernet oam profile	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM)	Attaches an Ethernet OAM profile to an interface.

dual-active exclude interface-vlan

To ensure that certain VLAN interfaces are not shut down on the virtual port-channel (vPC) secondary peer device when the vPC peer link fails for those VLANs carried on the vPC peer link but not by the vPC configuration, use the **dual-active exclude interface-vlan** command. To return to the default value, use the **no** form of this command.

dual-active exclude interface-vlan *range*
no dual-active exclude interface-vlan *range*

Syntax Description

<i>range</i>	Range of VLAN interfaces that you want to exclude from shutting down. The range is from 1 to 4094.
--------------	--

Command Default

None

Command Modes

vpc-domain configuration mode

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

Use the **dual-active exclude interface-vlan** command to ensure that those VLAN interfaces on the vPC secondary peer device that are carried on the vPC peer link but not by the vPC configuration do not go down if the vPC peer link fails. The VLAN interfaces must have already been configured.



Caution

We do not recommend that you configure an interface-VLAN exclude for a VLAN carried on a vPC because this action might cause packet losses on dual-active devices if the interface-VLAN still captures Layer 3 traffic while the vPC primary device and the vPC peer link are down.

This command does not require a license.

Examples

This example shows how to configure the device to keep the VLAN interfaces up on the vPC peer devices if the peer link fails:

```
switch# configure terminal
switch(config)# vpc-domain 5
switch(config-vpc-domain)# dual-active exclude interface-vlan 10
```

Related Commands

Command	Description
vpc-domain	Configures a vPC domain and enters the vpc-domain configuration mode.

duplex

To specify the duplex mode as full, half, or autonegotiate, use the **duplex** command. To return the system to default mode, use the **no** form of this command.

```
duplex {full | half | auto}
no duplex {full | half | auto}
```

Syntax Description

full	Specifies the duplex mode as full.
half	Specifies the duplex mode as half.
auto	Specifies the duplex mode as autonegotiate.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

The interface speed that you specify can affect the duplex mode used for an interface, so you should set the speed before setting the duplex mode. If you set the speed for autonegotiation, the duplex mode is automatically set to be autonegotiated. If you specify 10- or 100-Mbps speed, the port is automatically configured to use half-duplex mode, but you can specify full-duplex mode instead. Gigabit Ethernet is full duplex only. You cannot change the duplex mode on Gigabit Ethernet ports or on a 10/100/1000-Mbps port that is set for Gigabit Ethernet.

See the *Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide* Release 5.x for more information about interface speed and duplex settings.

This command does not require a license.

Examples

This example shows how to specify the duplex mode for full duplex:

```
switch(config-if)# duplex full
```

Related Commands

Command	Description
show interface	Displays information about the interface, which includes the duplex parameter.

dying-gasp

To configure what action is taken on an interface when a dying-gasp notification is received from the remote Ethernet OAM peer, use the **dying-gasp** command in Ethernet OAM action configuration mode or interface Ethernet OAM action configuration mode. To remove the configuration, use the **no** form of this command.

dying-gasp {**disable** | **error-disable-interface** | **log**}
no dying-gasp {**disable** | **error-disable-interface** | **log**}

Syntax Description		
disable	Performs no action on the interface when a dying-gasp notification is received.	
error-disable-interface	Puts the interface into the error-disable state when a dying-gasp notification is received.	
log	(Interface Ethernet OAM action configuration only) Creates a syslog entry when a dying-gasp notification is received. This action is available in Interface Ethernet OAM configuration mode to override the profile setting and log the event for the interface when it occurs.	

Command Default The default action is to create a syslog entry.

Command Modes Ethernet OAM action configuration (config-eoam-action)
 Interface Ethernet OAM action configuration (config-if-eoam-action)

Command History	Release	Modification
	7.3(0)D1(1)	This command was introduced.

Usage Guidelines This command does not require a license.

The following example shows how to configure that no action is performed on the interface when a dying-gasp notification is received.

```
switch# configure terminal
switch(config)# ethernet oam profile Profile_1
switch(config-eoam)# action
switch(config-eoam-action)# dying-gasp disable
```

The following example shows how to configure that the interface is put into the error-disable state when a dying-gasp notification is received.

```
switch# configure terminal
switch(config)# ethernet oam profile Profile_1
switch(config-eoam)# action
switch(config-eoam-action)# dying-gasp error-disable-interface
```

The following example shows how to configure that a syslog is created when a dying-gasp notification is received:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ethernet oam
```



```
switch(config-if-eoam)# action  
switch(config-if-eoam-action)# dying-gasp log
```

Related Commands

Command	Description
ethernet oam profile	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM)	Attaches an Ethernet OAM profile to an interface.



E Commands

- [encapsulation dot1Q](#), on page 60
- [errdisable detect cause](#), on page 61
- [errdisable recovery cause](#), on page 62
- [errdisable recovery interval](#), on page 64
- [ethernet oam](#), on page 65
- [ethernet oam profile](#), on page 66

encapsulation dot1Q

To enable IEEE 802.1Q encapsulation of traffic on a specified subinterface in a virtual LAN (VLAN), use the **encapsulation dot1q** command. To disable encapsulation, use the **no** form of this command.

encapsulation dot1Q vlan-id
no encapsulation dot1Q vlan-id

Syntax Description

<i>vlan-id</i>	VLAN to set when the interface is in access mode. The range is from 1 to 4094 except for the VLANs reserved for internal switch use.
----------------	--

Command Default

No encapsulation

Command Modes

Subinterface configuration mode

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

IEEE 802.1Q encapsulation is configurable on Ethernet interfaces. IEEE 802.1Q is a standard protocol for interconnecting multiple switches and routers and for defining VLAN topologies.

Use the **encapsulation dot1q** command in subinterface range configuration mode to apply a VLAN ID to the subinterface.

This command does not require a license.

Examples

This example shows how to enable dot1Q encapsulation on a subinterface for VLAN 30:

```
switch(config-subif)# encapsulation dot1q 30
```

Related Commands

Command	Description
show vlan dot1Q	Displays dot1Q encapsulation information for a VLAN.

errdisable detect cause

To enable error-disabled (errdisable) detection for an application, use the **errdisable detect cause** command. To return to the default setting, use the **no** form of this command.

```
errdisable detect cause {acl-exception | all | link-flap | loopback}
no errdisable detect cause {acl-exception | all | link-flap | loopback}
```

Syntax Description	Parameter	Description
	acl-exception	Enables error-disabled detection for access-list installation failures.
	all	Enables error-disabled detection on all causes.
	link-flap	Enables error-disabled detection on link-state flapping.
	loopback	Enables error-disabled detection on loopback.

Command Default Disabled

Command Modes Global configuration mode

Command History	Release	Modification
	4.0	This command was introduced.

Usage Guidelines Use the **errdisable detect cause** command to enable error detection for an application.

A cause is defined as the reason why the error-disabled state occurred. When a cause is detected on an interface, the interface is placed in an error-disabled state. This error-disabled state is an operational state that is similar to the link-down state. You must enter the **shutdown** command and then the **no shutdown** command to recover an interface manually from the error-disabled state.

This command does not require a license.

Examples

This example shows how to enable error-disabled detection on all cases:

```
switch(config)# errdisable detect cause all
```

Related Commands	Command	Description
	shutdown	Brings the port down administratively.
	no shutdown	Brings the port up administratively.
	err-disabled	Displays the interface error-disabled state.

errdisable recovery cause

To enable an automatic recovery from the error-disabled (errdisable) state for an application, use the **errdisable recovery cause** command. To return to the default setting, use the **no** form of this command.

```
errdisable recovery cause {all | bpduguard | link-flap | link-oam-discovery-timeout |
link-oam-dying-gasp | loopback | failed-port-state | psecure-violation | security-violation | storm-control
| uddl | vpc-peerlink}
no errdisable recovery cause {all | bpduguard | link-flap | loopback | failed-port-state | psecure-violation
| security-violation | storm-control | uddl | vpc-peerlink}
```

Syntax Description

all	Enables an automatic recovery from all causes.
bpduguard	Enables an automatic recovery from BPDU Guard error-disabled state.
loopback	Enables the timer to recover from loopback error-disabled state detected by UDLD.
failed-portstate	Enables a timer automatic recovery from the STP set port state failure.
link-flap	Enables an automatic recovery from link-state flapping.
link-oam-discovery-timeout	Enable timer to recover from Ethernet link OAM discovery timeout.
link-oam-dying-gasp	Enable timer to recover from Ethernet link OAM dying gasp.
psecure-violation	Enables a timer automatic recovery from the psecure violation disable state.
security-violation	Enables an automatic recovery from the 802.1X violation disable state.
storm-control	Enables an automatic recovery from the storm control error-disabled state.
uddl	Enables an automatic recovery from the UDLD error-disabled state.
vpc-peerlink	Enables an automatic recovery from an inconsistent virtual port channel (vPC) peer-link error-disabled state.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(2)	Added the loopback keyword.
4.1(3)	Added the vpc-peerlink parameter.
4.0	This command was introduced.

Usage Guidelines

Use the **errdisable recovery cause** command to enable an automatic recovery on the interface from the error-disabled state for an application. This command tries to bring the interface out of the error-disabled state

and retry operation once all the causes have timed out. The interface automatically tries to come up again after 300 seconds. To change this interval, use the **errdisable recovery interval** command.

This command does not require a license.

Examples

This example shows how to automatically recover from the error-disabled state for link flapping after you have enabled the recovery timer:

```
switch(config)# errdisable recovery cause link-flap
```

Related Commands

Command	Description
errdisable recovery interval	Enables the recovery timer.
show interface status err-disabled	Displays interface error-disabled state.

errdisable recovery interval

To enable the recovery timer, use the **errdisable recovery interval** command.

errdisable recovery interval *interval*

Syntax Description

<i>interval</i>	Error detection for access-list installation failures. The range is from 30 to 65535.
-----------------	---

Command Default

300 seconds

Command Modes

Global configuration mode

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **errdisable recovery interval** command to configure the recovery timer.

This command does not require a license.

Examples

This example shows how to configure the recovery timer:

```
switch(config)# errdisable recovery interval 32
```

Related Commands

Command	Description
errdisable recovery cause	Enables the error-disabled recovery for an application.
show interface status err-disabled	Displays the interface error-disabled state.

ethernet oam

To enable Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode, use the **ethernet oam** command in interface configuration mode. To disable Ethernet Link OAM, use the **no** form of this command.

ethernet oam
noethernet oam

This command has no keywords or arguments.

Command Default

None

Command Modes

Interface configuration (config-if)

Supported User Roles

network-admin
vdc---admin
network---operator
vdc-operator

Command History

Release	Modification
7.3(0)D1(1)	This command was introduced.

Usage Guidelines

When you enable Ethernet Link OAM on an interface, the default Ethernet Link OAM values are applied to the interface. For the default Ethernet Link OAM values, see the related Ethernet Link OAM commands.

This command does not require a license.

This example shows how to configure the connection timeout value of an Ethernet OAM session:

```
switch# configure terminal
switch(config)# interface ethernet 2/19
switch(config-eoam)# ethernet oam
switch(config-if-eoam)#
```

Related Commands

Command	Description
ethernet oam profile	Creates an EOAM profile and enters EOAM configuration mode.
show ethernet oam configuration	Displays the current active Ethernet OAM configuration on an interface.

ethernet oam profile

To create an Ethernet Operations, Administration and Maintenance (EOAM) profile and enter EOAM configuration mode, use the **ethernet oam profile** command in global configuration mode. To delete an EOAM profile, use the no form of this command.

ethernet oam profile *profile-name*
noethernet oam profile *profile-name*

Syntax Description	<i>profile-name</i> Text string name of the OAM profile. The maximum length is 32 bytes.
---------------------------	--

Command Default	None
------------------------	------

Command Modes	Global configuration (config)
----------------------	-------------------------------

Supported User Roles

network-admin
vdc--admin
network--operator
vdc-operator

Command History	Release	Modification
	7.3(0)D1(1)	This command was introduced.

Usage Guidelines Before you can delete an EOAM profile, you must remove the profile from all interfaces to which it is attached. This command does not require a license.

This example shows how to create an Ethernet OAM profile and enter Ethernet OAM configuration mode:

```
switch(config)# ethernet oam profile Profile_1
switch(config-eoam)#
```

Related Commands	Command	Description
	ethernet oam	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
	show ethernet oam configuration	Displays the current active Ethernet OAM configuration on an interface.



F Commands

- [fabricpath switch-id](#), on page 68
- [feature bfd](#), on page 69
- [feature ethernet-link-oam](#), on page 70
- [feature interface-vlan](#), on page 71
- [feature lacp](#), on page 72
- [feature tunnel](#), on page 73
- [feature udld](#), on page 74
- [feature vpc](#), on page 75
- [fec](#), on page 76
- [flowcontrol](#), on page 78
- [frame-period threshold](#), on page 80
- [frame-period window](#), on page 81
- [frame-seconds threshold](#), on page 82
- [frame-seconds window](#), on page 84
- [frame threshold](#), on page 85
- [frame window](#), on page 87

fabricpath switch-id

To configure an emulated switch ID, use the **fabricpath switch-id** command. To return to the default setting, use the **no** form of this command.

fabricpath switch-id *switch-id*
no fabricpath switch-id *switch-id*

Syntax Description	<i>switch-id</i> Emulated switch ID. The range is from 1 to 4095.
---------------------------	---

Command Default None

Command Modes Interface configuration mode

Command History	Release	Modification
	5.1(1)	This command was introduced.

Usage Guidelines This command does not require a license.

Examples This example shows how to configure an emulated switch ID:

```
switch# configure terminal
switch(config)# vpc domain 1
switch(config-vpc-domain)# fabricpath switch-id 4
Configuring fabricpath switch id will flap vPCs. Continue (yes/no)? [no] yes
Note:
-----:: Re-init of peer-link and vPCs started ::-----
switch(config-vpc-domain)#
```

This example shows how to set the default ID value:

```
switch# configure terminal
switch(config)# vpc domain 1
switch(config-vpc-domain)# no fabricpath switch-id 4
Deconfiguring fabricpath switch id will flap vPCs. Continue (yes/no)? [no] yes
Note:
-----:: Re-init of peer-link and vPCs started ::-----
switch(config-vpc-domain)#
```

Related Commands	Command	Description
	show interface switchport	Displays the administrative and operational status of a switching (nonrouting) port.

feature bfd

To enable Bidirectional Forwarding Detection (BFD), use the **feature bfd** command. To return to the default setting, use the **no** form of this command.

feature bfd
no feature bfd

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Global configuration mode

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines You must use the **feature bfd** command to enable the BFD functionality.



Note The device does not display any BFD commands until you enable the feature.

This command does not require a license.

Examples

This example shows how to enable BFD functionality on the device:

```
switch# configure terminal
switch(config)# feature bfd
switch(config)#
```

Related Commands	Command	Description
	show feature	Displays information about the features enabled on the device.

feature ethernet-link-oam

To enable the ethernet link OAM feature, use the **feature ethernet-link-oam** command in global configuration mode. To disable the ethernet link OAM feature, use the no form of this command.

feature ethernet-link-oam

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Global configuration (config)

Command History	Release	Modification
	7.3(0)D1(1)	This command was introduced.

Usage Guidelines This command does not require a license.

The following example shows how to enable the ethernet link OAM feature:

```
switch# configure terminal
switch(config)# feature ethernet-link-oam
```

Related Commands

Command	Description
ethernet oam profile	Creates an EOAM profile and enters EOAM configuration mode.

feature interface-vlan

To enable the creation of VLAN interfaces (switched virtual interfaces [SVI]), use the **feature interface-vlan** command. To disable the VLAN interface feature, use the **no** form of this command.

feature interface-vlan
no feature interface-vlan

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Global configuration mode

Release	Modification
4.0	This command was introduced.

Usage Guidelines You must use the **feature interface-vlan** command before you can create VLAN interfaces. This command does not require a license.

Examples This example shows how to enable the interface VLAN feature:

```
switch(config)# feature interface-vlan
```

Command	Description
interface vlan	Creates a VLAN interface.

feature lacp

To enable Link Aggregation Control Protocol (LACP) port channeling on the device, use the **feature lacp** command. To disable LACP on the device, use the **no** form of this command.

feature lacp
no feature lacp

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Global configuration mode

Release	Modification
4.0	This command was introduced.

Usage Guidelines You must remove all the LACP configuration parameters from all port channels on the device before you can disable LACP. You cannot disable LACP while LACP configurations remain on the device.

Even after you enable LACP globally, you do not have to run LACP on all port channels on the device. You enable LACP on each channel mode using the **channel-group mode** command.

When you enter the **no** form of this command, the system removes all the LACP configuration from the device.

This command does not require a license.

Examples This example shows how to enable LACP port channeling on the device:

```
switch(config)# feature lacp
```

Command	Description
show lacp port-channel	Displays information on port channels with LACP enabled.

feature tunnel

To enable the creation of tunnel interfaces, use the **feature tunnel** command. To disable the tunnel interface feature, use the **no** form of this command.

feature tunnel
no feature tunnel

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Global configuration mode

Command History	Release	Modification
	4.0	This command was introduced.

Usage Guidelines You must use the **feature tunnel** command before you can create tunnel interfaces. This command requires the Enterprise license.

Examples This example shows how to enable the interface tunnel feature:

```
switch(config)# feature tunnel
```

Related Commands	Command	Description
	interface tunnel	Creates a tunnel interface.

feature udd

To enable Unidirectional Link Detection (UDLD) globally on the device, use the **feature udd** command. To disable UDLD globally on the device, use the **no** form of this command.

feature udd
no feature udd

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Global configuration mode

Release	Modification
4.0	This command was introduced.

Usage Guidelines Use the **feature udd** command to enable UDLD globally on the device. UDLD must be also enabled on the other linked interface and its device. After enabling the devices, it is possible to enable a UDLD *mode* for an interface.

Use the **no feature udd** command to disable UDLD globally for Ethernet interfaces on the device.

This command does not require a license.

Examples

This example shows how to enable the UDLD for a device:

```
switch# configure terminal
switch(config)# feature udd
```

This example shows how to disable UDLD for a device:

```
switch# configure terminal
switch(config)# no feature udd
```

Related Commands

Command	Description
show udd	Displays information about the UDLD configuration.

feature vpc

To enable virtual port channels (vPCs), use the **feature vpc** command. To return to the default setting, use the **no** form of this command.

feature vpc
no feature vpc

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Global configuration mode

Command History	Release	Modification
	4.1(3)	This command was introduced.

Usage Guidelines You must use the **feature vpc** command to enable the vPC functionality. You must enable vPCs before you can configure them.



Note When you disable vPC, the device clears all the vPC configurations.

This command does not require a license.

Examples

This example shows how to enable vPC functionality on the device:

```
switch(config)#feature vpc
```

Related Commands	Command	Description
	show feature	Displays information about the features enabled on the device.
	show vpc brief	Displays vPC information on vPCs. If the feature is not enabled, the system displays an error when you enter this command.

fec

To configure the Forward Error Correction (FEC) feature for the interface range, use the **fec** command. To return to the default setting, use the **no** form of this command.

```
fec { auto | cl91 | off }
no fec
```

Syntax Description

auto	Enables the FEC feature based on the transceiver type.
cl91	Enables clause 91 for 100 Gigabit interface.
off	Disables FEC for the interface range.

Command Default

Disabled

Command Modes

Interface configuration mode

Command History

Release Modification

4.1(3) This command was introduced.

This example shows how to configure FEC feature on the device:

```
switch(config)# interface ethernet1/2
switch(config-if-range)# fec cl91
switch(config-if-range)# exit
switch(config)# copy running-config startup-config
switch(config)# exit
switch# show interface Ethernet1/2

Ethernet1/2 is up
admin state is up, Dedicated Interface
  Hardware: 40000/100000 Ethernet, address: 00e0.d50f.9fe0 (bia 00eb.d50e.9fe0)
  MTU 9216 bytes, BW 40000000 Kbit, DLY 10 usec
  reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, medium is broadcast
  Port mode is access
  full-duplex, 40 Gb/s, media type is 40G
  Beacon is turned off
  Auto-Negotiation is turned on
  Input flow-control is off, output flow-control is off
  Auto-mdix is turned off
  Rate mode is dedicated
  Switchport monitor is off
  EtherType is 0x8100
  EEE (efficient-ethernet) : n/a
    admin fec state is auto, oper fec state is off
  .
  .
  .
```

Related Commands

Command	Description
show feature	Displays information about the features enabled on the device.

flowcontrol

To enable or disable the ability of the Ethernet port to send and receive flow-control pause frames, use the **flowcontrol** command. To return to the default flow-control settings, use the **no** form of this command.

flowcontrol {send | receive} {desired | on | off}

no flowcontrol {send | receive}

Syntax Description

send	Specifies the flow-control send setting for ports that run at 1000 Mbps or faster.
receive	Specifies the flow-control receive setting for ports that run at any speed.
desired	Specifies the remote port setting to desired for both send and receive, if the configuration of the remote port is unknown.
on	Specifies the remote port setting to on, if you want the local port to send flow-control pause frames.
off	Specifies the remote port's send and receive parameter settings to off, if you do not want to use flow control.

Command Default

1-Gb/s interfaces—Off for receive and send

10-Gb/s interfaces—Off for receive and send

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the flowcontrol command to enable or disable the ability of the Ethernet port to send and receive flow-control pause frames.

Make sure that the remote port has the corresponding setting for the flow control that you need. If you want the local port to send flow-control pause frames, the remote port has a receive parameter set to on or desired. If you want the local port to receive flow-control frames, you must make sure that the remote port has a send parameter set to on or desired. If you do not want to use flow control, you can set the remote port's send and receive parameters to off.

For Ethernet ports that run at 1 Gbps or faster speeds, you can enable or disable the port's ability to send and receive flow-control pause frames. For Ethernet ports that run slower than 1 Gbps, you can enable or disable only the port's ability to receive pause frames.

When enabling flow control for the local port, you either fully enable the local port to send or receive frames regardless of the flow-control setting of the remote port or you set the local port to use the desired setting used by the remote port. If you enable both the local and remote ports for flow control, set the desired flow control of the other port, or set a combination of those two states, flow control is enabled for those ports.



Note For ports that run at 10 Gbps, you cannot use the desired state for the send or receive parameter. The **desired** keyword in the **flowcontrol** command is not supported for higher port speeds such as 40 Gb/s and 100 Gb/s.

To see how the different port flow-control states affect the link flow-control state, see [Table 2: Port Flow-Control Influences on Link Flow Control, on page 79](#).

Table 2: Port Flow-Control Influences on Link Flow Control

Port Flow Control States	Link Flow Control State	
Port Receiving Data (Sends Pause Frames)	Port Transmitting Data (Receives Pause Frames)	
Enabled	Enabled	Enabled
Enabled	Desired	Enabled
Enabled	Disabled	Disabled
Desired	Enabled	Enabled
Desired	Desired	Enabled
Desired	Disabled	Disabled
Disabled	Enabled	Disabled
Disabled	Desired	Disabled
Disabled	Disabled	Disabled

This command does not require a license.

Examples

This example shows how to set Ethernet port 3/1 to send flow-control pause frames:

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# flowcontrol send on
```

Related Commands

Command	Description
show interface	Displays information about the interface, which includes the flow-control parameter.
show interface flowcontrol	Displays information about the interface flow control.

frame-period threshold

To configure the thresholds that trigger an Ethernet OAM frame-period error event, use the **frame-period threshold** command in Ethernet OAM link monitor or interface Ethernet OAM link monitor configuration mode. To remove the configuration, use the **no** form of this command.

```
frame-period threshold low threshold [high threshold]  
no frame-period threshold [low threshold [high threshold]]
```

Syntax Description	
	low <i>threshold</i> Low threshold, in frames, that triggers a frame-period error event. The range is 1 to 1000000. The default value for low threshold is 60000.
	(Optional) high <i>threshold</i> High threshold, in frames, that triggers a frame-period error event. The range is 1 to 1000000. The high threshold value can be configured only in conjunction with the low threshold value.

Command Default The default low threshold value is 1. There is no default high threshold value.

Command Modes Ethernet OAM link monitor configuration (config-eoam-lm)
Interface Ethernet OAM link monitor configuration (config-if-eoam-lm)

Supported User Roles

network-admin
vdc---admin
network---operator
vdc-operator

Command History	Release	Modification
	7.3(0)D1(1)	This command was introduced.

Usage Guidelines When the low threshold is passed, a frame-period error event notification is generated and transmitted to the OAM peer. Additionally, any registered higher level OAM protocols, such as Connectivity Fault Management (CFM), are also notified. When the high threshold is passed, the configured high threshold action is performed in addition to the low threshold actions. The high threshold is optional and is configurable only in conjunction with the low threshold.

This command does not require a license.

The following example shows how to configure the low and high thresholds that trigger a frame-period error event.

```
switch(config)# ethernet oam profile Profile_1  
switch(config-eoam)# link-monitor  
switch(config-eoam-lm)# frame-period threshold low 100 high 600000
```


frame-period window

To configure the window size for an Ethernet OAM frame-period error event, use the **frame-period window** command in Ethernet OAM link monitor or interface Ethernet OAM link monitor configuration mode. To remove the configuration, use the **no** form of this command.

frame-period window *window*
no frame-period window [*window*]

Syntax Description	<i>window</i> Size of the window for a frame-period error in milliseconds. The range is 1000 to 60000.
---------------------------	--

Command Default	The default window size value is 1000.
------------------------	--

Command Modes	Ethernet OAM link monitor configuration (config-eoam-lm) Interface Ethernet OAM link monitor configuration (config-if-eoam-lm)
----------------------	---

Supported User Roles

network-admin
vdc---admin
network---operator
vdc-operator

Command History	Release	Modification
	7.3(0)D1(1)	This command was introduced.

Usage Guidelines	This command does not require a license.
-------------------------	--

Task ID	Task ID	Operation
----------------	----------------	------------------

The following example shows how to configure the window size for a frame-period error:

```
switch(config)# ethernet oam profile Profile_1
switch(config-eoam)# link-monitor
switch(config-eoam-lm)# frame-period window 60000
```

frame-seconds threshold

To configure the thresholds that trigger a frame-seconds error event, use the **frame-seconds threshold** command in Ethernet OAM link monitor or interface Ethernet OAM link monitor configuration mode. To remove the configuration, use the **no** form of this command.

```
frame-seconds threshold low threshold [high threshold]  
no frame-seconds threshold [low threshold [high threshold]]
```

Syntax Description	low <i>threshold</i> Low threshold, in seconds, that triggers a frame-seconds error event. The range is 1 to 900.
	high <i>threshold</i> (Optional) High threshold, in seconds, that triggers a frame-seconds error event. The range is 1 to 900. The high threshold value can be configured only in conjunction with the low threshold value.

Command Default The default low threshold value is 1. There is no default high threshold value.

Command Modes Ethernet OAM link monitor configuration (config-eoam-lm)
Interface Ethernet OAM link monitor configuration (config-if-eoam-lm)

Supported User Roles

network-admin
vdc---admin
network---operator
vdc-operator

Command History	Release	Modification
	7.3(0)D1(1)	This command was introduced.

Usage Guidelines When the low threshold is passed, a frame-seconds error event notification is generated and transmitted to the OAM peer. Additionally, any registered higher level OAM protocols, such as Connectivity Fault Management (CFM), are also notified. When the high threshold is passed, the configured high threshold action is performed in addition to the low threshold actions. The high threshold is optional and is configurable only in conjunction with the low threshold.

This command does not require a license.

The following example shows how to configure the low and high thresholds that trigger a frame-seconds error event:

```
switch(config)# ethernet oam profile Profile_1  
switch(config-eoam)# link-monitor  
switch(config-eoam-lm)# frame-seconds threshold low 10 high 900
```

Related Commands

Command	Description
ethernet oam profile	Creates an EOAM profile and enters EOAM configuration mode.
link-monitor	Enters Ethernet OAM link monitor configuration mode.

frame-seconds window

To configure the window size for the OAM frame-seconds error event, use the **frame-seconds window** command in Ethernet OAM link monitor or interface Ethernet OAM link monitor configuration mode. To remove the configuration, use the **no** form of this command.

```
frame-seconds window window
no frame-seconds window [window]
```

Syntax Description	<i>window</i> Size of the window for a frame-seconds error in milliseconds. The range is 10000 to 900000.
---------------------------	---

Command Default	The default window size value is 60000.
------------------------	---

Command Modes	Ethernet OAM link monitor configuration (config-eoam-lm) Interface Ethernet OAM link monitor configuration (config-if-eoam-lm)
----------------------	---

Supported User Roles

```
network-admin
vdc--admin
network---operator
vdc-operator
```

Command History	Release Modification
	7.3(0)D1(1) This command was introduced.

Usage Guidelines	This command does not require a license.
-------------------------	--

The following example shows how to configure the window size for a frame-seconds error.

```
switch(config)# ethernet oam profile Profile_1
switch(config-eoam)# link-monitor
switch(config-eoam-lm)# frame-seconds window 900000
```

Related Commands

Command	Description
ethernet oam profile	Creates an EOAM profile and enters EOAM configuration mode.
link-monitor	Enters Ethernet OAM link monitor configuration mode.

frame threshold

To configure the thresholds that trigger an Ethernet OAM frame error event, use the **frame threshold** command in Ethernet OAM link monitor or interface Ethernet OAM link monitor configuration mode. To remove the configuration, use the **no** form of this command.

```
frame threshold low threshold [high threshold]
no frame threshold low threshold [high threshold]
```

Syntax Description	<p>lowthreshold Low threshold, in symbols, that triggers a frame error event. The range is 1 to 12000000.</p> <p>lowthreshold (Optional) High threshold, in symbols, that triggers a frame error event. The range is 1 to 12000000. The high threshold value can be configured only in conjunction with the low threshold value.</p>				
Command Default	The default low threshold value is 1. There is no default high threshold value.				
Command Modes	<p>Ethernet OAM link monitor configuration (config-eoam-lm)</p> <p>Interface Ethernet OAM link monitor configuration (config-if-eoam-lm)</p>				
Supported User Roles	<p>network-admin</p> <p>vdc---admin</p> <p>network--operator</p> <p>vdc-operator</p>				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>7.3(0)D1(1)</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	7.3(0)D1(1)	This command was introduced.
Release	Modification				
7.3(0)D1(1)	This command was introduced.				

Usage Guidelines

When the low threshold is passed, a frame error event notification is generated and transmitted to the OAM peer. Additionally, any registered higher level OAM protocols, such as Connectivity Fault Management (CFM), are also notified. When the high threshold is passed, the configured high threshold action is performed in addition to the low threshold actions. The high threshold is optional and is configurable only in conjunction with the low threshold.

This command does not require a license.

The following example shows how to configure the low and high thresholds that trigger a frame error event:

```
switch(config)# ethernet oam profile Profile_1
switch(config-eoam)# link-monitor
switch(config-eoam-lm)# frame threshold low 100 high 60000
```

Related Commands

Command	Description
ethernet oam profile	Configures collection parameters for a Bulkstat data group. Creates an EOAM profile and enters EOAM configuration mode.
link-monitor	Enters Ethernet OAM link monitor configuration mode.

frame window

To configure the frame window size of an OAM frame error event, use the **frame window** command in Ethernet OAM link monitor or interface Ethernet OAM link monitor configuration mode. To remove the configuration, use the **no** form of this command.

frame window *window*
no frame window [*window*]

Syntax Description	<i>window</i> Size of the window for a frame error in seconds. The range is 1000 to 60000.
---------------------------	--

Command Default	The default frame window size is 1000.
------------------------	--

Command Modes	Ethernet OAM link monitor configuration (config-eoam-lm) Interface Ethernet OAM link monitor configuration (config-if-eoam-lm)
----------------------	---

Command History	Release Modification
	7.3(0)D1(1) This command was introduced.

Usage Guidelines	This command does not require a license.
-------------------------	--

The following example shows how to configure the window size for a frame error.

```
switch(config)# ethernet oam profile Profile_1
switch(config-eoam)# link-monitor
switch(config-eoam-lm)# frame window 60
```

Related Commands	Command	Description
	ethernet oam profile	Creates an EOAM profile and enters EOAM configuration mode.
	link-monitor	Enters Ethernet OAM link monitor configuration mode.



G Commands

- [graceful consistency-check, on page 90](#)

graceful consistency-check

To enable a graceful type-1 consistency check on per VLAN basis, use the **graceful consistency-check** command. To disable the graceful consistency check, use the **no** form of this command.

graceful consistency-check
no graceful consistency-check

Syntax Description This command has no arguments or keywords.

Command Default Enabled

Command Modes VPC domain configuration mode (config-vpc-domain)

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines This command does not require a license.

Examples

This example shows how to enable the graceful type-1 consistency check:

```
switch# configure terminal
switch(config)# vpc domain 1
switch(config-vpc-domain)# graceful consistency-check
switch(config-vpc-domain)#
```

This example shows how to disable the graceful type-1 consistency check:

```
switch# configure terminal
switch(config)# vpc domain 1
switch(config-vpc-domain)# no graceful consistency-check
switch(config-vpc-domain)#
```

Command	Description
vpc	Moves other port channels into the vPC.
vpc domain	Creates a vPC domain.



H Commands

- [high-threshold](#), on page 92
- [hsrp bfd](#), on page 94

high-threshold

To configure what action is taken on an interface when a high threshold is exceeded, use the **high-threshold** command in Ethernet OAM action configuration mode or interface Ethernet OAM action configuration mode. To remove the configuration, use the **no** form of this command.

high-threshold {**disable** | **error-disable-interface** | **log**}
no high-threshold {**disable** | **error-disable-interface** | **log**}

Syntax Description		
disable	(Interface Ethernet OAM action configuration only) Overrides the profile setting and takes no action at the interface when a high threshold is exceeded.	
error-disable-interface	Puts the interface into the error-disable state when a high threshold is exceeded.	
log	Creates a syslog entry when a high threshold is exceeded.	

Command Default No action is taken when a high threshold is exceeded.

Command Modes Ethernet OAM action configuration (config-eoam-action)
 Interface Ethernet OAM action configuration (config-if-eoam-action)

Command History	Release	Modification
	7.3(0)D1(1)	This command was introduced.

Usage Guidelines This command does not require a license.

The following example shows how to configure that a syslog entry is created on the interface when a high threshold is exceeded:

```
switch# configure terminal
switch(config)# ethernet oam profile Profile_1
switch(config-eoam)# action
switch(config-eoam-action)# high-threshold log
```

The following example shows how to configure that the interface is put into the error-disable state when a high threshold is exceeded:

```
switch# configure terminal
switch(config)# ethernet oam profile Profile_1
switch(config-eoam)# action
switch(config-eoam-action)# high-threshold error-disable-interface
```

The following example shows how to configure that no action is taken when a high threshold is exceeded:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ethernet oam
switch(config-if-eoam)# action
switch(config-if-eoam-action)# high-threshold disable
```

Related Commands

Command	Description
ethernet oam profile	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM)	Attaches an Ethernet OAM profile to an interface.

hsrp bfd

To enable Bidirectional Forwarding Detection (BFD) on a Hot Standby Router Protocol (HSRP) interface, use the **hsrp bfd** command. To return to the default setting, use the **no** form of this command.

```
hsrp bfd
no hsrp bfd
```

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Interface configuration mode

Command History	Release	Modification
	5.0(2)	This command was introduced.

Usage Guidelines Use the **hsrp bfd** command to enable BFD on an HSRP interface. This command does not require a license.

Examples This example shows how to enable BFD for an HSRP interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# hsrp bfd
```

Related Commands	Command	Description
	feature bfd	Enables the BFD feature.



I Commands

- [inherit port-profile, on page 96](#)
- [interface cmp-mgmt module, on page 98](#)
- [interface ethernet, on page 99](#)
- [interface loopback, on page 100](#)
- [interface mgmt, on page 101](#)
- [interface port-channel, on page 102](#)
- [interface tunnel, on page 104](#)
- [interface vlan, on page 105](#)
- [ip eigrp bfd, on page 106](#)
- [ip ospf bfd, on page 107](#)
- [ip pim bfd-instance, on page 108](#)
- [ip pim bfd, on page 109](#)
- [ipv6 eigrp bfd, on page 110](#)
- [isis bfd, on page 111](#)

inherit port-profile

To assign a port profile to an interface or range of interfaces and to inherit an additional port profile onto an existing port profile, use the **inherit port-profile** command. To remove an inherited port profile or to remove a port profile from specified interfaces, use the **no** form of this command.

inherit port-profile *name*
no inherit port-profile *name*

Syntax Description	<i>name</i> Port profile that you want to assign to interfaces or to inherit onto the existing port profile.
---------------------------	--

Command Default None

Command Modes Interface configuration modePort-profile configuration mode

Command History	Release	Modification
	4.2(1)	This command was introduced.

Usage Guidelines Use the **inherit port-profile** command to do the following:

- Assign the port profile to a specified interface or range of specified interfaces. You do this action in the interface configuration mode. The maximum number of interfaces that can inherit a single profile is 512.
- Inherit configuration parameters from another port profile onto an existing port profile. You do this action in the port-profile mode, using the name of the port profile that you want to inherit configurations into. Only port profiles of the same type can be inherited by another port profile. The device supports four levels of inheritance except for the **switchport private-vlan mapping** and the **private-vlan mapping** commands, which support only one inheritance level. The same port profile can be inherited by any number of port profiles. In a port-profile inheritance hierarchy, all the profiles must have the same switchport configuration.

See the **port-profile** command and the **state-enabled** command for information about creating, configuring, and enabling port profiles.

If you attempt to inherit a port profile to the wrong type of interface, the system returns an error.

When you remove a port profile from a range of interfaces, the system undoes the configuration from the interfaces first and then removes the port-profile link. Also, when you remove a port profile, the system checks the interface configuration and either skips port-profile commands that have been overridden by directly entered interface commands or returns the command to the default value.

You can also choose a subset of interfaces from which to remove a port profile from those interfaces to which you originally applied the profile. For example, if you configured a port profile and configured 10 interfaces to inherit that port profile, you can remove the port profile from just some of the specified 10 interfaces. The port profile continues to operate on the remaining interfaces to which it is applied.

You use the port-profile configuration mode to remove an inherited port profile from an original port profile.

This command does not require a license.

Examples

This example shows how to assign a specified port profile to a range of interfaces:

```
switch(config)# interface ethernet 2/1-10  
switch(config-if)# port-profile test
```

This example shows how to inherit the configuration parameters from the port profile named switch onto the port profile named test:

```
switch(config)# test  
switch(config-ppm)# inherit port-profile switch
```

Related Commands

Command	Description
show port-profile	Displays information about port profiles.

interface cmp-mgmt module

To create a Connectivity Management Processor (CMP) management interface and enter interface configuration mode, use the **interface cmp-mgmt module** command.

interface cmp-mgmt module *number*

Syntax Description	<i>number</i> Active or standby supervisor module number. Valid values are 9 or 10.
---------------------------	---

Command Default	None
------------------------	------

Command Modes	Global configuration mode Interface configuration mode
----------------------	---

Command History	Release	Modification
	4.0	This command was introduced.

Usage Guidelines	Use the interface cmp-mgmt module command to create a CMP management interface. This command does not require a license.
-------------------------	--

Examples	This example shows how to create a CMP management interface:
-----------------	--

```
switch(config)# interface cmp-mgmt module 9
switch(config-if-cmp)#
```

interface ethernet

To configure an Ethernet interface and enter interface configuration mode, use the **interface ethernet** command.

interface ethernet *slot/port-list*

Syntax Description	<i>slot/port-list</i>	Slot number and port list for the Ethernet interface. The range is from 1 to 253 for slots and from 1 to 128 for ports.
---------------------------	-----------------------	---

Command Default None

Command Modes Global configuration mode
Interface configuration mode

Command History	Release	Modification
	4.0	This command was introduced.

Usage Guidelines Use the **interface ethernet** command to enter the interface configuration mode for the specified interface or range of interfaces.



Note *slot/port-list* is a space-separated list of slots and ports.

This command does not require a license.

Examples

This example shows how to enter the interface command mode for the Ethernet interface on slot 2, port 1:

```
switch(config)# interface ethernet 2/1
switch(config-if)#
```

Related Commands	Command	Description
	show interface ethernet	Displays information about the Ethernet interface.

interface loopback

To create a loopback interface and enter interface configuration mode, use the **interface loopback** command. To remove a loopback interface, use the **no** form of this command.

interface loopback *number*
no interface loopback *number*

Syntax Description

<i>number</i>	Interface number. The range is from 0 to 1023.
---------------	--

Command Default

None

Command Modes

Global configuration mode

Interface configuration mode

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **interface loopback** command to create or modify loopback interfaces.

This command does not require a license.

Examples

This example shows how to create a loopback interface:

```
switch(config)# interface loopback 50
switch(config-if)#
```

Related Commands

Command	Description
show interface loopback	Displays information about the traffic on the specified loopback interface.

interface mgmt

To configure the management interface and enter interface configuration mode, use the **interface mgmt** command.

interface mgmt *number*

Syntax Description

<i>number</i>	Interface number. The range is from 0 to 1023.
---------------	--

Command Default

None

Command Modes

Global configuration mode

Interface configuration mode

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **interface mgmt** command to configure the management interface and to enter the interface configuration mode.

This command does not require a license.

Examples

This example shows how to enter the interface configuration mode to configure the management interface:

```
switch(config)# interface mgmt
switch(config-if)#
```

Related Commands

Command	Description
show interface mgmt0	Displays information about the traffic on the management interface.

interface port-channel

To create a port-channel interface and enter interface configuration mode, use the **interface port-channel** command. To remove a logical port-channel interface or subinterface, use the **no** form of this command.

interface port-channel *channel-number*
no interface port-channel *channel-number*

Syntax Description

<i>channel-number</i>	Channel number that is assigned to this port-channel logical interface. The range is from 1 to 4096.
-----------------------	--

Command Default

None

Command Modes

Global configuration mode

Interface configuration mode

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **interface port-channel** command to create or delete port-channel groups and to enter the interface configuration mode for the port channel.

You can create port channels implicitly using the auto-recovery command or explicitly using the feature tunnel command.

A port can belong to only one channel group.

You can create subinterfaces on a Layer 3 port-channel interface. However, you cannot add a Layer 3 interface that has existing subinterfaces to a port channel.



Note The Layer 3 port-channel interface is the routed interface.

The Link Aggregation Control Protocol (LACP) system ID is unique for each virtual device context (VDC), and channel-group numbers and names can be reused in different VDCs.

When you use the **interface port-channel** command, follow these guidelines:

- If you are using the Cisco Discovery Protocol (CDP), you must configure it only on the physical interface and not on the port-channel interface.
- If you do not assign a static MAC address on the port-channel interface, a MAC address is automatically assigned. If you assign a static MAC address and then later remove it, the MAC address is automatically assigned.
- The MAC address of the port channel is the address of the first operational port added to the channel group. If this first-added port is removed from the channel, the MAC address comes from the next operational port added, if there is one.

This command does not require a license.

Examples

This example shows how to create a port-channel group interface with channel-group number 50:

```
switch(config)# interface port-channel 50  
switch(config-if)#
```

Related Commands

Command	Description
show lacp	Displays LACP information.
show interface port-channel	Displays information on traffic on the specified port-channel interface.
show port-channel summary	Displays information on the port channels.

interface tunnel

To create a tunnel interface and enter interface configuration mode, use the **interface tunnel** command. To remove a tunnel interface, use the **no** form of this command.

interface tunnel *number-list*
no interface tunnel *number-list*

Syntax Description

<i>number-list</i>	Identifying interface number list. The range is from 0 to 4095.
--------------------	---

Command Default

None

Command Modes

Global configuration mode
 Interface configuration mode

Command History

Release	Modification
5.0(1)	The maximum valid range of values was changed from 65535 to 4095.
4.0	This command was introduced.

Usage Guidelines

Use the **interface tunnel** command to create or modify tunnel interfaces.

Cisco NX-OS supports the generic routing encapsulation (GRE) header defined in IETF RFC 2784. Cisco NX-OS does not support tunnel keys and other options from IETF RFC 1701.

You can configure IP tunnels only in the default virtual device context (VDC).



Note number-list is a space-separated list of tunnels.

This command requires the Enterprise license.

Examples

This example shows how to create a tunnel interface:

```
switch(config)# interface tunnel 50
switch(config-if)#
```

Related Commands

Command	Description
show interface tunnel	Displays information about the traffic on the specified tunnel interface.
tunnel destination	Sets the destination of the IP tunnel.
tunnel source	Sets the source of the IP tunnel.

interface vlan

To create a VLAN interface and enter interface configuration mode, use the **interface vlan** command. To remove a VLAN interface, use the **no** form of this command.

interface vlan *vlan-id*
no interface vlan *vlan-id*

Syntax Description	<i>vlan-id</i> VLAN to set when the interface is in access mode. The range is from 1 to 4094, except for the VLANs reserved for the internal switch use.
---------------------------	--

Command Default None

Command Modes Global configuration mode
 Interface configuration mode

Command History	Release	Modification
	4.0	This command was introduced.

Usage Guidelines Use the **interface vlan** command to create or modify VLAN interfaces.

The VLAN interface is created the first time that you enter the **interface vlan** command for a particular VLAN. The *vlan-id* argument corresponds to the VLAN tag that is associated with the data frames on an Inter-Switch Link (ISL), the IEEE 802.1Q-encapsulated trunk, or the VLAN ID that is configured for an access port.

This command does not require a license.

Examples This example shows how to create a VLAN interface for VLAN 50:

```
switch(config)# interface vlan 50
switch(config-if)#
```

Related Commands	Command	Description
	feature interface-vlan	Enables the ability to create VLAN interfaces.
	show interface vlan	Displays information about the traffic on the specified VLAN interface.

ip eigrp bfd

To enable Bidirectional Forwarding Detection (BFD) on an Enhanced Interior Gateway Routing Protocol (EIGRP) interface, use the **ip eigrp bfd** command. To return to the default setting, use the **no** form of this command.

ip eigrp instance-tag bfd
no ip eigrp instance-tag bfd

Syntax Description

<i>instance-tag</i>	EIGRP instance tag. The instance tag can be any case-sensitive, alphanumeric string up to 20 characters.
---------------------	--

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

Use the **ip eigrp bfd** command to enable BFD on an EIGRP interface. This command takes precedence over the **bfd** command in router configuration mode.

This command does not require a license.

Examples

This example shows how to enable BFD for an EIGRP interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ip eigrp Test1 bfd
```

Related Commands

Command	Description
bfd	Enables BFD on all EIGRP interfaces.
feature bfd	Enables the BFD feature.

ip ospf bfd

To enable Bidirectional Forwarding Detection (BFD) on an Open Shortest Path First version 2 (OSPFv2) interface, use the **ip ospf bfd** command. To return to the default setting, use the **no** form of this command.

ip ospf bfd
no ip ospf bfd

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Interface configuration mode

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines Use the **ip ospf bfd** command to enable BFD on an OSPFv2 interface. This command takes precedence over the **bfd** command in router configuration mode.

This command does not require a license.

Examples This example shows how to enable BFD for an OSPF interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ip ospf bfd
```

Related Commands

Command	Description
bfd	Enables BFD on all OSPFv2 interfaces.
feature bfd	Enables the BFD feature.

ip pim bfd-instance

To enable Bidirectional Forwarding Detection (BFD) for Protocol Independent Multicast (PIM) on an interface, use the **ip pim bfd-instance** command. To return to the default setting, use the **no** form of this command.

ip pim bfd-instance [**disable**]
no ip pim bfd-instance [**disable**]

Syntax Description	disable (Optional) Disables BFD for PIM on this interface.
---------------------------	---

Command Default None

Command Modes Interface configuration mode

Command History	Release	Modification
	5.0(2)	This command was introduced.

Usage Guidelines Use the **ip pim bfd-instance** command to enable BFD for PIM on an interface. This configuration (with or without the **disable** keyword) overrides the BFD configuration for PIM at the global or VRF configuration level.

This command does not require a license.

Examples This example shows how to disable BFD for PIM on interface ethernet 2/1 when BFD is enabled globally for PIM:

```
switch# configure terminal
switch(config)# ip pim bfd
switch(config)# interface ethernet 2/1
switch(config-if)# ip pim bfd-instance disable
```

Related Commands	Command	Description
	feature bfd	Enables the BFD feature.

ip pim bfd

To enable Bidirectional Forwarding Detection (BFD) for Protocol Independent Multicast (PIM), use the **ip pim bfd** command. To return to the default setting, use the **no** form of this command.

```
ip pim bfd
no ip pim bfd
```

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Global configuration mode

Command History	Release	Modification
	5.0(2)	This command was introduced.

Usage Guidelines Use the **ip pim bfd** command to enable BFD for PIM. This command does not require a license.

Examples This example shows how to enable BFD for PIM:

```
switch# configure terminal
switch(config)# ip pim bfd
```

Related Commands	Command	Description
	feature bfd	Enables the BFD feature.

ipv6 eigrp bfd

To enable Bidirectional Forwarding Detection (BFD) on an Enhanced Interior Gateway Routing Protocol (EIGRP), use the **ipv6 eigrp bfd** command. To return to the default setting, use the **no** form of this command.

ipv6 eigrp instance-tag bfd
no ipv6 eigrp instance-tag bfd

Syntax Description

<i>instance-tag</i>	EIGRP instance tag. The instance tag can be any case-sensitive, alphanumeric string up to 20 characters.
---------------------	--

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

Use the **ipv6eigrpbfd** command to enable BFD on an EIGRP interface. This command takes precedence over the **bfd** command in router configuration mode.

This command does not require a license.

Examples

This example shows how to enable BFD for an EIGRP interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 eigrp Test1 bfd
```

Related Commands

Command	Description
bfd	Enables BFD on all EIGRP interfaces.
feature bfd	Enables the BFD feature.

isis bfd

To enable Bidirectional Forwarding Detection (BFD) on an Intermediate System-to-Intermediate System (IS-IS) interface, use the **isis bfd** command. To return to the default setting, use the **no** form of this command.

isis [ipv6] bfd
no isis bfd

Syntax Description

<i>ipv6</i>	(Optional) Enables IPv6 BFD on a specific interface that is configured for IS-IS.
-------------	---

Command Default

None

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
6.2(2)	Added the ipv6 keyword to the syntax description.
5.0(2)	This command was introduced.

Usage Guidelines

Use the **isis bfd** command to enable BFD on an IS-IS interface. This command takes precedence over the **bfd** command in router configuration mode.

This command does not require a license.

Examples

This example shows how to enable BFD for an IS-IS interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# isis ipv6 bfd
switch(config-if)#
```

Related Commands

Command	Description
bfd	Enables BFD on all IS-IS interfaces.
feature bfd	Enables the BFD feature.



L Commands

- [l2protocol tunnel](#), on page 114
- [l2protocol tunnel cos](#), on page 115
- [l2protocol tunnel drop-threshold](#), on page 116
- [l2protocol tunnel shutdown-threshold](#), on page 117
- [lacp graceful-convergence](#), on page 118
- [lacp max-bundle](#), on page 120
- [lacp min-links](#), on page 121
- [lacp port-priority](#), on page 122
- [lacp rate](#), on page 123
- [lacp suspend-individual](#), on page 124
- [lacp system-priority](#), on page 126
- [layer3 peer-router](#), on page 127
- [link-monitoring](#), on page 128
- [link debounce](#), on page 129
- [link-monitor](#), on page 131
- [load-interval](#), on page 132

l2protocol tunnel

To enable Layer 2 protocol tunneling, use the **l2protocol tunnel** command. To disable protocol tunneling, use the **no** form of this command.

l2protocol tunnel [{**cdp** | **stp** | **vtp**}]
no l2protocol tunnel [{**cdp** | **stp** | **vtp**}]

Syntax Description

cdp	(Optional) Enables Cisco Discovery Protocol (CDP) tunneling.
stp	(Optional) Enables Spanning Tree Protocol (STP) tunneling.
vtp	(Optional) Enables VLAN Trunking Protocol (VTP) tunneling.

Command Default

Layer 2 protocol tunneling is disabled.

Command Modes

Interface configuration mode

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to enable Layer 2 protocol tunneling:

```
switch(config-if)# l2protocol tunnel cdp
```

Related Commands

Command	Description
show l2protocol tunnel	Displays Layer 2 protocol tunnel information.

l2protocol tunnel cos

To specify a global class of service (CoS) value on all Layer 2 protocol tunneling interfaces, use the **l2protocol tunnel cos** command. To reset the global CoS value to its default, use the **no** form of this command.

l2protocol tunnel cos *cos-value*
no l2protocol tunnel cos

Syntax Description

<i>cos-value</i>	CoS value. The range is from 0 to 7. The default value is 5.
------------------	--

Command Default

CoS value is 5.

Command Modes

Global configuration mode

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to specify a global CoS value on all Layer 2 protocol tunneling interfaces:

```
switch(config)# l2protocol tunnel cos 7
```

Related Commands

Command	Description
show l2protocol tunnel	Displays Layer 2 protocol tunnel information.

l2protocol tunnel drop-threshold

To specify the maximum number of packets that can be processed on a Layer 2 protocol tunneling interface before being dropped, use the **l2protocol tunnel drop-threshold** command. To reset the values to 0 and disable the drop threshold, use the **no** form of this command.

l2protocol tunnel drop-threshold [{**cdp** | **stp** | **vtp**}] *packets-per-sec*
no l2protocol tunnel drop-threshold [{**cdp** | **stp** | **vtp**}]

Syntax Description

cdp	(Optional) Specifies the number of Cisco Discovery Protocol (CDP) packets that can be processed on an interface.
stp	(Optional) Specifies the number of Spanning Tree Protocol (STP) packets that can be processed on an interface.
vtp	(Optional) Specifies the number of VLAN Trunking Protocol (VTP) packets that can be processed on an interface.
<i>packets-per-sec</i>	Maximum number of packets that can be processed on an interface before being dropped. The range is from 1 to 4096.

Command Default

The drop threshold is disabled.

Command Modes

Interface configuration mode

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to specify the maximum number of CDP packets that can be processed on an Layer 2 protocol tunneling interface before being dropped:

```
switch(config-if)# l2protocol tunnel drop-threshold cdp 1024
```

Related Commands

Command	Description
show l2protocol tunnel	Displays Layer 2 protocol tunnel information.

l2protocol tunnel shutdown-threshold

To specify the maximum number of packets that can be processed on a Layer 2 protocol tunneling interface, use the **l2protocol tunnel shutdown-threshold** command. To reset the values to 0 and disable the shutdown threshold, use the **no** form of this command

```
l2protocol tunnel shutdown-threshold [{cdp | stp | vtp}] packets-per-sec
no l2protocol tunnel shutdown-threshold [{cdp | stp | vtp}]
```

Syntax Description	cdp	(Optional) Specifies the number of Cisco Discovery Protocol (CDP) packets that can be processed on an interface.
	stp	(Optional) Specifies the number of Spanning Tree Protocol (STP) packets that can be processed on an interface.
	vtp	(Optional) Specifies the number of VLAN Trunking Protocol (VTP) packets that can be processed on an interface.
	<i>packets-per-sec</i>	Maximum number of packets that can be processed on an interface. When the number of packets is exceeded, the port is put in error-disabled state. The range is from 1 to 4096.

Command Default The shutdown threshold is disabled.

Command Modes Interface configuration mode

Command History	Release	Modification
	5.0(2)	This command was introduced.

Usage Guidelines When the number of packets is exceeded, the port is put in error-disabled state. This command does not require a license.

Examples This example shows how to specify the maximum number of packets that can be processed on an Layer 2 protocol tunneling interface before the port is put in error-disabled state:

```
switch(config-if)# l2protocol tunnel shutdown-threshold 2048
```

Related Commands	Command	Description
	show l2protocol tunnel	Displays Layer 2 protocol tunnel information.

lACP graceful-convergence

To configure Link Aggregation Control Protocol (LACP) graceful convergence on a port channel or vPC physical port, use the **lACP graceful-convergence** command. To disable graceful convergence, use the **no** form of this command.

lACP graceful-convergence
no lACP graceful-convergence

Syntax Description This command has no arguments or keywords.

Command Default Enabled.

Command Modes Interface configuration
 vpc configuration mode

Release	Modification
7.1(1)D1(0)	This command can be configured on a vPC physical port.
4.2(3)	This command was introduced.

Usage Guidelines Use the **no lACP graceful-convergence** command only with LACP ports that are connected to a non-Nexus peer. Using the **no lACP graceful-convergence** command with a Cisco Nexus peer may cause port suspension.



Note The port channel has to be in the administratively down state before the **lACP graceful-convergence** or the **no lACP graceful-convergence** command can be run.

To allow LACP graceful convergence on the vPC physical port, the device must be in vpc configuration mode (config-if-vpc).

This command does not require a license.

Examples

This example shows how to configure LACP graceful convergence the port channel:

```
switch(config)# interface port-channel 2
switch(config-if)# shutdown
switch(config-if)# lACP graceful-convergence
switch(config-if)# no shutdown
```

This example shows how to configure LACP graceful convergence the vPC physical port:

```
switch(config)# interface ethernet1/1
switch(config-if)# vpc 1
switch(config-if-vpc)# lACP graceful-convergence
```

Command	Description
show lACP summary	Displays information summary information about LACP.

Command	Description
show vpc brief	Displays brief information about the vPCs.

lacp max-bundle

To configure a port channel maximum bundle, use the **lacp max-bundle** command. To return to the default setting, use the **no** form of this command.

lacp max-bundle *max-bundle-number*
no lacp mac-bundle *max-bundle-number*

Syntax Description

<i>max-bundle-number</i>	Maximum bundle number. The range is from 1 to 16.
--------------------------	---

Command Default

The default for the port channel max-bundle is 16.

The allowed range is from 1 to 16.

Command Modes

Interface configuration mode

Command History

Release	Modification
5.1(1)	This command was introduced.

Usage Guidelines



Note Even if the default value is 16, the number of active members in a port channel is the minimum number of the maximum bundle configured and the maximum active members that are allowed in the portchannel.

This command does not require a license.

Examples

This example shows how to configure port channel maximum bundles:

```
switch(config)# interface port-channel 1
switch(config-if)# lacp max-bundle 2
switch(config-if)#
```

Related Commands

Command	Description
interface	Enters the interface configuration mode and configures the types and identities of interfaces.

lacp min-links

To configure the minimum links for a port channel, use the **lacp min-links** command. To return to the default setting, use the **no** form of this command.

lacp min-links *number*
no lacp min-links *number*

Syntax Description

<i>number</i>	Minimum link number. The range is from 1 to 16.
---------------	---

Command Default

The default for the port channel minimum link is 1.
 The allowed range is from 1 to 16.

Command Modes

Interface configuration mode

Command History

Release	Modification
5.1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure the minimum link for a port channel:

```
switch(config)# interface port-channel 1
switch(config-if)# lacp min-links 3
switch(config-if)#
```

Related Commands

Command	Description
interface	Enters the interface configuration mode and configures the types and identities of interfaces.

lacp port-priority

To set the priority for the physical interfaces for the Link Aggregation Control Protocol (LACP), use the **lacp port-priority** command. To return the port priority to the default value, use the **no** form of this command.

lacp port-priority *priority*

no lacp port-priority

Syntax Description

<i>priority</i>	Priority for the physical interfaces. The range is from 1 to 65535.
-----------------	---

Command Default

32768

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Each port configured to use LACP has an LACP port priority. You can accept the default value of 32768 for the LACP port priority, or you can configure a value between 1 and 65535. LACP uses the port priority with the port number to form the port identifier. The port priority is used to decide which ports should be put into standby mode when there is a hardware limitation that prevents all compatible ports from aggregating or when you have more than eight ports configured for the channel group.

When setting the priority, note that a *higher* number means a *lower* priority.

This command does not require a license.

Examples

This example shows how to set the LACP port priority for the interface to 2000:

```
switch(config-if)# lacp port-priority 2000
```

Related Commands

Command	Description
show lacp	Displays LACP information.

lACP rate

To set the rate at which the Link Aggregation Control Protocol (LACP) sends LACP control packets to an LACP-supported interface, use the **lACP rate** command. To reset the rate to its default, use the **no** form of this command.

```
lACP rate {fast | normal}
no lACP rate {fast | normal}
```

Syntax Description	fast	normal
	Specifies the fast rate of 1 second.	Specifies the default rate of 30 seconds.

Command Default 30 seconds

Command Modes Interface configuration mode

Command History	Release	Modification
	5.1(1)	This command was introduced.

Usage Guidelines You can change the LACP timer rate to modify the duration of the LACP timeout. Use the **lACP rate** command to set the rate at which LACP control packets are sent to an LACP-supported interface. You can change the timeout rate from the default rate (30 seconds) to the fast rate (1 second).

This command is supported only on LACP-enabled interfaces.

This command does not require a license.

Examples

This example shows how to configure the LACP fast rate on Ethernet interface 1/4:

```
switch# configure terminal
switch (config)# interface ethernet 1/4
switch(config-if)# lACP rate fast
```

Related Commands	Command	Description
	show lACP	Displays LACP information.

lACP suspend-individual

To enable LACP individual port suspension behavior on the port channel or vPC physical port, use the **lACP suspend-individual** command. To disable LACP individual port suspension behavior, use the **no** form of this command.

lACP suspend-individual
no lACP suspend-individual

Syntax Description This command has no arguments or keywords.

Command Default Enabled.

Command Modes Interface configuration
 vpc configuration mode

Release	Modification
7.1(1)D1(0)	This command can be configured on a vPC physical port.
4.2(3)	This command was introduced.

Usage Guidelines By default, LACP sets a port or vPC physical port to the suspended state if it does not receive an LACP PDU from the peer. In some cases, although this feature helps in preventing loops created due to misconfigurations, it can cause servers to fail to boot up because they require LACP to logically bring up the port. You can put a port or vPC physical port into an individual state by using the **lACP suspend-individual** command.



Note The port channel has to be in the administratively down state before the **lACP suspend-individual** or the **no lACP suspend-individual** command can be run.

To put the vPC physical port into an individual state, the device must be in vpc configuration mode (config-if-vpc).

This command does not require a license.

Examples

This example shows how to configure LACP graceful convergence the port channel:

```
switch(config)# interface port-channel 2
switch(config-if)# shutdown
```

```
switch(config-if-vpc)# lACP graceful-convergence
```

This example shows how to configure LACP graceful convergence the vPC physical port:

```
switch(config)# interface ethernet1/1
switch(config-if)# vpc 1
switch(config-if-vpc)# lACP graceful-convergence
```

Related Commands

Command	Description
show lacp summary	Displays information summary information about LACP.
show vpc brief	Displays brief information about the vPCs.

lACP system-priority

To set the system priority of the device for the Link Aggregation Control Protocol (LACP), use the **lACP system-priority command**. To return the system priority to the default value, use the **no** form of this command.

lACP system-priority *priority*
no lACP system-priority

Syntax Description

<i>priority</i>	Priority for the physical interfaces. The range is from 1 to 65535 .
-----------------	--

Command Default

32768

Command Modes

Global configuration mode

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Each device that runs LACP has an LACP system priority value. You can accept the default value of 32768 for this parameter, or you can configure a value between 1 and 65535. LACP uses the system priority with the MAC address to form the system ID and also during negotiation with other systems. The system ID is unique for each virtual device context (VDC).

When setting the priority, note that a *higher* number means a *lower* priority.

This command does not require a license.

Examples

This example shows how to set the LACP system priority for the device to 2500:

```
switch(config)# lACP system-priority 2500
switch(config)#
```

Related Commands

Command	Description
show lACP	Displays LACP information.
show lACP system identifier	Displays information on the LACP system identifier.

layer3 peer-router

To enable support for layer 3 routing protocols over virtual port channels (vPCs), use the **layer3 peer-router** command. To disable support for layer 3 routing protocols, use the **no** form of this command.

layer3 peer-router
no layer3 peer-router

Syntax Description This command has no arguments or keywords.

Command Default Disabled.

Command Modes VPC domain configuration mode

Command History	Release	Modification
	7.1(1)D1(0)	This command was introduced.

Usage Guidelines When you configure this command, the TTL value of packets destined to the vPC peer is not decremented. This command enables vPC to use layer 3 routing protocols that source packets with a TTL of 1.



Note This command is supported on F2, F2e, and F3 Series modules.

This command does not require a license.

Examples

This example shows how to enable support for layer 3 routing protocols over vPCs:

```
switch# configure terminal
switch(config)# vpc domain 1
(config-vpc-domain)# layer3 peer-router
```

Related Commands	Command	Description
	show vpc brief	Displays information about vPCs.

link-monitoring

To require that link-monitoring feature is configured on a remote switch before the OAM session is active, use the **link-monitoring** command in ethernet OAM require-remote configuration mode. To remove the requirement, use the **no** form of this command.

link-monitoring
no link-monitoring

Syntax Description	This command has no keywords or arguments.
Command Default	None
Command Modes	Ethernet OAM require-remote configuration (config-eoam-require)

Command History	Release	Modification
	7.3(0)D1(1)	This command was introduced.

Usage Guidelines This command does not require a license.

The following example shows how to set up a configuration to require that the link-monitoring feature is configured on a remote switch before the OAM session is active:

```
switch# configure terminal
switch(config)# feature ethernet-link-oam
switch(config)# ethernet oam profile Profile_1
switch(config-eoam)# require-remote
switch(config-eoam-require)# link-monitoring
```

Related Commands

Command	Description
ethernet oam profile	Creates an EOAM profile and enters EOAM configuration mode.
feature ethernet-link-oam	Enables the ethernet link OAM feature.
require-remote	Enters the ethernet OAM require-remote configuration submode to specify the features that you have to enable before an OAM session can become active.

link debounce

To enable the debounce timer for Ethernet ports and specify a debounce time, use the **link debounce** command. To disable the timer, use the **no** form of this command.

link debounce [{link-up | time}] [*milliseconds*]
no link debounce

Syntax Description		
link-up <i>milliseconds</i>	(Optional) Specifies the debounce link-up timer for the time you want to specify. The range is from 0 to 5000.	
time <i>milliseconds</i>	(Optional) Specifies the debounce timer for the time you want to specify. The range is from 0 to 5000.	

Command Default Enabled
 300 milliseconds

Command Modes Interface configuration mode

Command History	Release	Modification
	4.0	This command was introduced.
	7.3(0)D1(1)	The link-up keyword was added.

Usage Guidelines Use the link debounce command to enable the debounce timer for Ethernet ports and set it for a specified amount of time in milliseconds. The default debounce time applies when you enter the **link debounce** command with no arguments.

The range of time is from 1 to 5000 ms. The debounce timer is disabled if you specify the time to 0 ms.

This command does not require a license.

Examples

This example shows how to enable the debounce timer and set the debounce time to 1000 ms for the Ethernet port 3/1:

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# link debounce time 1000
```

This example shows how to configure the debounce link-up timer to 1000 ms for the Ethernet port 3/1:

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# link debounce link-up time 1000
```

This example shows how to disable the debounce timer for the Ethernet port 3/1:

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# no link debounce
```

Related Commands

Command	Description
show interface debounce	Displays the debounce time information about the interface.

link-monitor

To enter Ethernet OAM link monitor configuration mode, use the **link-monitor** command in Ethernet OAM configuration mode. To enter interface Ethernet OAM link monitor configuration mode, use the **link-monitor** command in interface Ethernet OAM configuration mode.

link-monitor

Syntax Description

This command has no keywords or arguments.

Command Default

None.

Command Modes

Ethernet OAM configuration (config-eoam)

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
---------	--------------

7.3(0)D1(1)	This command was introduced.
-------------	------------------------------

Usage Guidelines

This command does not require a license.

This example shows how to enter the Ethernet OAM link monitor configuration mode.

```
switch# configure terminal
switch(config)# ethernet oam profile Profile_1
switch(config-eoam)# link-monitorswitch(config-eoam-lm)#
```

The following example shows how to enter the link monitor configuration mode from interface Ethernet OAM configuration mode.

```
switch# configure terminal
switch(config)# interface ethernet 2/19
switch(config-if)# ethernet oam
switch(config-if-eoam)# link-monitor
```

load-interval

To change the sampling interval for statistics collections on interfaces, use the **load-interval** command. To return to the default sampling interval, use the **no** form of this command.

load-interval [**counter** {**1** | **2** | **3**}] *seconds*
no load-interval [**counter** {**1** | **2** | **3**}] [*seconds*]

Syntax Description

counter	(Optional) Specifies the counter for this load interval.
1 / 2 / 3	Specifies the counter number configured on the interface.
<i>seconds</i>	Interval between sampling statistics on the interface. The range is from 60 to 300 seconds for VLAN network interfaces, and the range is from 30 to 300 seconds for Ethernet and port-channel interfaces.

Command Default

1—30 seconds; 60 seconds for VLAN network interface
 2—300 seconds
 3—not configured

Command Modes

Interface configuration mode

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

Use the **load-interval** command to obtain bit-rate and packet-rate statistics for three different durations.

You can set the statistics collection intervals on the following types of interfaces:

- Ethernet interfaces
- Port-channel interfaces
- VLAN network interfaces

You cannot use this command on the management interface or subinterfaces.

This command sets the sampling interval for such statistics as packet rate and bit rate on the specified interface.

This command does not require a license.

Examples

This example shows how to set the three sample intervals for the Ethernet port 3/1:

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# load-interval counter 1 60
switch(config-if)# load-interval counter 2 135
switch(config-if)# load-interval counter 3 225
```

Related Commands

Command	Description
show interface	Displays information about the interface.
clear counters interface	Clears the counters for all load intervals for the specified interfaces.



M Commands

- [max-ports](#), on page 136
- [mdix auto](#), on page 137
- [medium](#), on page 138
- [mode auto](#), on page 139
- [mode \(Ethernet OAM\)](#), on page 140
- [mode \(require-remote\)](#), on page 141
- [mtu](#), on page 142

max-ports

To assign a maximum possible number of interfaces that a port profile can inherit, use the **max-ports** command. To return to the default value, use the **no** form of this command.

max-ports *number*
no max-ports *number*

Syntax Description

<i>number</i>	Maximum number of interfaces that a port profile can inherit. The range is from 1 to 512, and there is no default value.
---------------	--

Command Default

None

Command Modes

Port-profile configuration mode

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

You must be in the port-profile configuration mode in order to use this command.

You must enable each specific port profile by using the **state-enabled** command.

This command does not require a license.

Examples

This example shows how to enter the port-profile configuration mode and to configure the maximum possible number of interfaces that a port profile can inherit:

```
switch(config)# port-profile type ethernet type test
switch(config-ppm)# max-ports 500
```

Related Commands

Command	Description
show port-profile	Displays information about port profiles.
state-enabled	Enables a specified port profile.

mdix auto

To enable automatic medium-dependent independent crossover (MDIX) detection for the interface, use the **mdix auto** command. To turn automatic detection off, use the **no** form of this command.

mdix auto
no mdix

Syntax Description This command has no arguments or keywords.

Command Default Enabled

Command Modes Interface configuration mode

Command History	Release	Modification
	4.0	This command was introduced.

Usage Guidelines Use the **mdix auto** command to enable automatic MDIX detection for the port. Use the **no mdix** command to disable MDIX detection for the port.

This command is only available on copper Ethernet ports. To detect the type of connection (crossover or straight) with another copper Ethernet port, enable the MDIX parameter for the local port. Before you begin, MDIX must be enabled on the remote port.

This command does not require a license.

Examples

This example shows how to enable MDIX for Ethernet port 3/1:

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# mdix auto
```

This example shows how to disable MDIX for Ethernet port 3/1:

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# no
mdix
```

Related Commands	Command	Description
	show interface	Displays information about the interface, which includes the MDIX status.

medium

To set the medium mode for an interface, use the **medium** command. To remove the entry, use the **no** form of this command.

```
medium {broadcast | p2p}
no medium {broadcast | p2p}
```

Syntax Description

broadcast	Configures the interface as a broadcast medium.
p2p	Configures the interface as a point-to-point medium.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

The **medium** command is used to configure the interface as broadcast or point to point. This command does not require a license.

Examples

This example shows how to configure the interface for point-to-point medium:

```
switch(config-if)# medium p2p
```

mode auto

To enable specific commands for virtual port channels (vPCs) simultaneously, use the **mode auto** command.

mode auto

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes VPC domain configuration mode

Command History	Release	Modification
	6.2(2)	This command was introduced.

Usage Guidelines None

Examples

This example shows how to enable specific commands for vPCs simultaneously:

```
switch# configure terminal
switch(config)# vpc domain 1
switch(config-vpc-domain)# mode auto
The following commands are executed:
peer-gateway ;
auto-recovery ;
ip arp synchronize ;
ipv6 nd synchronize ;
fabricpath multicast load-balance ;
Warning:
Enables restoring of vPCs in a peer-detached state after reload, will wait for 240 seconds
to determine if peer is un-reachable
switch(config-vpc-domain)#
```

Related Commands	Command	Description
	show bfd clients	Displays the BFD client list.

mode (Ethernet OAM)

To configure the Ethernet OAM mode on an interface, use the **mode** command in Ethernet OAM or interface Ethernet OAM configuration mode. To return to the default, use the **no** form of the command.

```
mode {active | passive}
no mode [{active | passive}]
```

Syntax Description

passive Specifies that the interface operates in passive mode, where it cannot initiate the discovery process, generate a retrieval PDU, or request loopback.

active (Interface Ethernet OAM configuration only) Specifies that the interface operates in active mode to initiate processes and make requests.

Command Default

Active mode

Command Modes

Ethernet OAM configuration (config-eoam)
Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
7.3(0)D1(1)	This command was introduced.

Usage Guidelines

If a profile exists on the interface, setting the mode with this command overrides the mode setting in the profile on an interface.

This command does not require a license.

The following example shows how to enable Ethernet OAM passive mode on an Ethernet interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/19
switch(config-if)# ethernet oam
switch(config-if-eoam)# profile Profile_1
switch(config-if-eoam)# mode passive
```

Related Commands

Command	Description
ethernet oam profile	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam	Attaches an Ethernet OAM profile to an interface.
show ethernet oam configuration	Enables a Bulkstat profile for collection and transfer of data. Displays the current active Ethernet OAM configuration on an interface.
show ethernet oam interfaces	Displays the current state of Ethernet OAM interfaces.

mode (require-remote)

To require that an active or passive OAM mode is configured on a remote switch before the OAM session is active, use the **mode** command in ethernet OAM require-remote configuration mode. To remove the requirement, use the **no** form of this command.

```
mode {active | passive}
no mode [{active | passive}]
```

Syntax Description	active Requires that active mode is configured.				
	passive Requires that passive mode is configured.				
Command Default	None				
Command Modes	Ethernet OAM require-remote configuration (config-eoam-require)				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>7.3(0)D1(1)</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	7.3(0)D1(1)	This command was introduced.
Release	Modification				
7.3(0)D1(1)	This command was introduced.				
Usage Guidelines	This command does not require a license.				

The following example shows how to set up a configuration to require that passive mode is configured on a remote switch before the OAM session is active:

```
switch# configure terminal
switch(config)# feature ethernet-link-oam
switch(config)# ethernet oam profile Profile_1
switch(config-eoam)# require-remote
switch(config-eoam-require)# mode passive
```

Related Commands	Command	Description
	ethernet oam profile	Creates an EOAM profile and enters EOAM configuration mode.
	featureethernet-link-oam	Enables the ethernet link OAM feature.
	require-remote	Enters the ethernet OAM require-remote configuration submode to specify the features that you have to enable before an OAM session can become active.

mtu

To configure the maximum transmission unit (MTU) size for Layer 2 and Layer 3 Ethernet interfaces, use the **mtu** command. To return to the default value, use the **no** form of this command.

mtu *size*

no mtu

Syntax Description

<i>size</i>	For a Layer 2 interface, specify either the default MTU size (1500) in bytes or the system jumbo MTU size (9216, unless you have changed the default system jumbo size). For a Layer 3 interface, specify any even number between the range of 576 and 9216.
-------------	--

Command Default

1500 bytes

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **mtu** *size* command to configure the MTU size for Layer 2 and Layer 3 Ethernet interfaces.

For Layer 3 interfaces, you can configure the MTU to be between 576 and 9216 bytes (even values are required). For Layer 2 interfaces, you can configure the MTU to be either the system default MTU (1500 bytes) or the system jumbo MTU size (which has the default size of 9216 bytes).



Note

You can change the system jumbo MTU size, but if you change that value, you should also update the Layer 2 interfaces that use that value so that they use the new system jumbo MTU value. If you do not update the MTU value for Layer 2 interfaces, those interfaces use the system default MTU (1500 bytes).

This command does not require a license.

Examples

This example shows how to configure the Layer 2 Ethernet port 3/1 with the default MTU size (1500):

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# mtu 1500
```

Related Commands

Command	Description
show interface	Displays information about the interface, which includes the MTU size.



0 Commands

- [ospfv3 bfd, on page 144](#)

ospfv3 bfd

To configure Bidirectional Forwarding Detection (BFD) for Open Shortest Path First version 3 (OSPFv3) on one or more interfaces, use the **ospfv3 bfd** command.

ospfv3 bfd [**disable**]

Syntax Description

disable	(Optional) Enables BFD on a per-interface basis for one or more interfaces associated with the OSPFv3 routing process.
----------------	--

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

OSPFv3 must be running on all participating devices. You must configure the baseline parameters for BFD sessions on the interfaces over which you want to run BFD sessions to discover BFD neighbors.

Examples

This example shows how to configure BFD for OSPFv3 on one or more interfaces:

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-router)# ospfv3 bfd disable
switch(config-if)# exit
switch(config)#
```

Related Commands

Command	Description
show ospfv3	Displays information about OSPFv3 routing processes.



P Commands

- [peer-gateway](#), on page 146
- [peer-keepalive destination](#), on page 147
- [peer-switch](#), on page 151
- [port-channel limit](#), on page 152
- [port-channel load-balance](#), on page 154
- [port-channel load-balance hash-modulo](#), on page 156
- [port-channel load-defer](#), on page 157
- [port-profile](#), on page 158
- [profile \(EOAM\)](#), on page 161

peer-gateway

To configure the device to send virtual port-channel (vPC) packets to the device's MAC address, use the **peer-gateway** command. To return to the default value, use the **no** form of this command.

```
peer-gateway
no peer-gateway
```

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes vpc-domain configuration mode

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines Use the **peer-gateway** command to have a vPC peer device act as the gateway even for packets that are sent to the vPC peer device's MAC address.

This command does not require a license.

Examples

This example shows how to configure the device to use the switch gateway even for the packets that are sent to the vPC:

```
switch# configure terminal
switch(config)# vpc-domain 5
switch(config-vpc-domain)# peer-gateway
```

Command	Description
vpc-domain	Configures a vPC domain and enters the vpc-domain configuration mode.

peer-keepalive destination

To configure the virtual port-channel (vPC) peer-keepalive link and message between vPC peer devices, use the **peer-keepalive destination** command.

```
peer-keepalivedestination ipaddress [hold-timeout secs] [interval msecs {timeout secs} {precedence | {prec-value | network | internet | critical | flash-override | flash | immediate | priority | routine}} | {tos | {tos-value | max-reliability | max-throughput | min-delay | min-monetary-cost | normal}} | tos-byte tos-byte-value] [source ip address] [udp-port number] [vrf {name | management | vpc-keepalive}]
```

Syntax Description

<i>ip address</i>	IP address of the remote vPC peer device. Note You can either enter an IPv4 or IPv6 address.
hold-timeout <i>secs</i>	(Optional) Specifies when the peer-keepalive link goes down, the secondary vPC peer device waits the hold-timeout interval. The range is from 3 to 10. During the hold-timeout, the vPC secondary device does not take any action based on any keepalive messages received, because the keepalive might be received just temporarily, such as if a supervisor fails a few seconds after the peer link goes down.
interval <i>msecs</i>	Specifies the number of milliseconds that you want between sending keepalive messages to the remote vPC peer device. This variable configures the interval between sending peer-keepalive messages to the remote vPC peer device and the maximum period to wait to receive a keepalive message from the remote vPC peer device. The range is from 400 to 10,000.
timeout <i>secs</i>	(Optional) Specifies that the timeout timer starts at the end of the hold-timeout interval. During the timeout period, the secondary vPC peer device checks for vPC peer-keepalive hello messages from the primary vPC peer device. If the secondary vPC peer device receives a single hello message, that device disables all vPC interfaces on the secondary vPC peer device. The range is from 3 and 20. During the timeout, the vPC secondary device takes action to become the vPC primary device if no keepalive message is received by the end of the configured interval.

precedence <i>prec-value</i>	(Optional) Specifies the precedence value for the peer-keepalive message. Valid values are as follows: <ul style="list-style-type: none"> • 0 to 7 • network (7) • internet (6) • critical (5) • flash-override (4) • flash (3) • immediate (2) • priority (1) • routine (0)
tos tos-value	(Optional) Specifies the precedence or ToS value for the peer-keepalive message. Valid values are as follows: <ul style="list-style-type: none"> • 0, 1, 2, 4, 8 • max-reliability (2) • max-throughput (4) • min-delay (8) • min-monetary-cost (1) • normal (0) <p>Note The only valid values are shown here.</p>
tos-byte	(Optional) Specifies the precedence, or 8-bit ToS value, for the peer-keepalive message. A higher numerical value indicates the higher throughput priority. The range is from 0 to 255.
source	(Optional) Specifies the IP address of the local vPC peer device. Note Must be an IPv4 address.
<i>number</i>	(Optional) Number of the UDP port to send and receive the vPC peer-keepalive messages. The range is from 1024 to 6500.
<i>name</i>	(Optional) Name of the virtual routing and forwarding (VRF) instance that you want to use for the vPC peer-keepalive link and messages.
vrf vrf-name	(Optional) Specifies a VRF instance.
management	(Optional) Specifies the management interface.
vpc-keepalive	(Optional) Specifies a vPC keepalive.

Command Default

Peer-keepalive is disabled.
 Hold-timeout is 3 seconds.
 Interval is 1000 milliseconds.
 Timeout is 5 seconds.
 Precedence is default, with a level of 6 (internet).
 UDP port is 3200.
 VRF is management VRF.

Command Modes

vpc-domain configuration mode

Command History

Release	Modification
4.1(3)	This command was introduced.

Usage Guidelines

You must enable the vPC feature before you can configure the peer-keepalive parameters. The vPC keepalive messages notify the system if one of the vPC peer devices goes down.

You must configure the peer-keepalive messages on each of the vPC peer devices to enable the functionality.

Although the keepalive messages can transmit over any Layer 3 topology, we recommend that you create and configure a separate VRF with Layer 3 ports on each vPC peer device as the source and destination for the vPC keepalive messages. The default ports and VRF for the peer-alive link are the management ports and the management VRF. Do not use the peer link itself for the vPC peer-keepalive messages.

Ensure that both the source and destination IP addresses used for the peer-keepalive messages are unique in your network.

The vPC keepalive messages are IP/UDP messages.

This command accepts only IPv4 addresses.

The device assumes that its vPC peer device is down when the device does not receive any messages from the peer during the timeout period. We recommend that you configure the timeout value to be three times the interval value.

You can configure either the **precedence**, **tos**, or **tos-byte** value to ensure throughput for the vPC peer-keepalive message.

**Note**

We recommend that you create a separate VRF and assign a Layer 3 port on each vPC peer device for the peer-keepalive link.

This command does not require a license.

Examples

This example shows how to configure the IP address of the remote vPC peer device for the fault-tolerant link:

```
switch(config-vpc-domain)# peer-keepalive destination 172.28.231.85
```

Related Commands

Command	Description
show running-config vpc all	Displays information on the vPC peer-keepalive status. If the feature is not enabled, the system displays an error when you enter this command.
show vpc peer-keepalive	Displays information on the vPC peer-keepalive status. If the feature is not enabled, the system displays an error when you enter this command.

peer-switch

To enable the virtual port channel (vPC) switch pair to appear as a single Spanning Tree Protocol (STP) root in the Layer 2 topology, use the **peer-switch** command. To disable the peer switch vPC topology, use the **no** form of this command.

peer-switch
no peer-switch

Syntax Description This command has no arguments or keywords.

Command Default Peer switch Layer 2 topology is disabled.

Command Modes vPC domain configuration mode

Command History	Release	Modification
	5.0(2)	This command was introduced.

Usage Guidelines This command does not require a license.

Examples

This example shows how to enable the vPC switch pair to appear as a single STP root in the Layer 2 topology:

```
switch(config)# vpc domain 5
switch(config-vpc-domain)# peer-switch
2010 Apr 28 14:44:44 switch %STP-2-VPC_PEERSWITCH_CONFIG_ENABLED: vPC peer-switch
configuration is enabled. Please make sure to configure spanning tree "bridge" priority as
per recommended guidelines to make vPC peer-switch operational.
```

Related Commands	Command	Description
	vpc domain	Creates a virtual port-channel (vPC) domain.

port-channel limit

To configure more than 244 virtual port channels (vPCs), use the **port-channel limit** command. To disable this feature, use the **no** form of this command.

port-channel limit
no port-channel limit

Syntax Description This command has no arguments or keywords.

Command Default Limit to 244 vPCs

Command Modes vPC domain configuration

Command History

Release	Modification
6.1(2)E1	This command was introduced.

Usage Guidelines

To enable this command, first enter the fabricpath multicast load-balance command.

Following guidelines when using the no port-channel limit command:

- Entering this command causes the peer links and vPCs to go up and down and could cause traffic losses.
- Only F2 series modules support this configuration. It cannot be configured on VDCs that do not have an F2 series module.
- Entering this command changes FabricPath MAC addresses that are used by vPC+ port channels. It leads to some transient flooding until the MAC addresses are learned again.
- In-service software upgrades (ISSUs) and In-service software downgrades (ISSDs) are not supported.
- Remove the no port-channel limit configuration before attempting an ISSD to an image that does not support this configuration. To revert to an earlier configuration, the number of vPCs that you must be 244 or less.
- To unconfigure the FabricPath multicast load-balance configuration, you must first remove the no port-channel limit configuration.

This command does not require a license.

Examples

This example shows how to configure the maximum number of supported vPCs:

```
switch# switchto vdc peer1
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2012, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
```



```

http://www.opensource.org/licenses/lgpl-2.1.php
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch-peer1(config)# vpc domain 1
switch(config-vpc-domain)# port-channel limit
switch(config-vpc-domain)# no port-channel limit
switch(config-vpc-domain)#

```

This example shows how to configure no port-channel limit:

```

switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# vpc domain 1
switch(config-vpc-domain)# fabricpath multicast load-balance
switch(config-vpc-domain)# no port-channel limit
switch(config-vpc-domain)#

```

This example shows how to enable support of more than 244 vPC+ port channels:

```

switch1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch1(config)# vpc domain 1
switch1(config-vpc-domain)# fabricpath multicast load-balance
switch1(config-vpc-domain)# no port-channel limit

```

Related Commands

Command	Description
show vpc brief	Displays a brief status of the vPC.

port-channel load-balance

To set the load-balancing method among the interfaces in the channel-group bundle, use the **port-channel load-balance** command. To return the system priority to the default value, use the **no** form of this command.

port-channel load-balance *method* [**module** *slot*]
noport-channel load-balance *method* [**module** *slot*]

Syntax Description

<i>method</i>	Load-balancing method. See the “Usage Guidelines” section for a list of valid values.
module <i>slot</i>	(Optional) Specifies the module slot number.

Command Default

Layer 2 packets—**src-dst-mac**
 Layer 3 packets—**src-dst-ip**

Command Modes

Global configuration mode

Command History

Release	Modification
6.2(2)	Added the new method “vlan-only” which is applicable at the module level (for F2/F2e modules only).
5.1(3)	The word ethernet was removed from the command name.
4.0	This command was introduced.

Usage Guidelines

When you do not specify a module, you are configuring load balancing for the entire device. When you use the module parameter, you are configuring load balancing for the specified modules.

A load-balance hash will be effective on the egress module only when the desired load-balance hash is configured on the ingress module also. So make sure that you configure the desired port-channel load-balance hash on the module where the traffic ingresses.

Valid *method* values are as follows:

- **dst-ip**—Loads distribution on the destination IP address.
- **dst-mac**—Loads distribution on the destination MAC address.
- **dst-port**—Loads distribution on the destination port.
- **src-dst-ip**—Loads distribution on the source XOR-destination IP address.
- **src-dst-mac**—Loads distribution on the source XOR-destination MAC address.
- **src-dst-port**—Loads distribution on the source XOR-destination port.
- **src-ip**—Loads distribution on the source IP address.
- **src-mac**—Loads distribution on the source MAC address.
- **src-port**—Loads distribution on the source port.

- `vlan-only`—Loads distribution on the vlan modules only.



Note You cannot configure load balancing using port channels per virtual device context (VDC). You must be in the default VDC to configure this feature; if you attempt to configure this feature from another VDC the system returns an error.

Use the **module** keyword to configure the module independently for port-channeling and load-balancing mode. The remaining module uses current load-balancing method configured for the entire device or the default method if you have not configured a method for the entire device. When you enter the **no** form with the **module** keyword, the load-balancing method for the specified module takes the current load-balancing method that is in use for the entire device. If you configured a load-balancing method for the entire device, the specified module uses that configured method rather than the default **src-dst-ip/src-dst-mac**. The per-module configuration takes precedence over the load-balancing method configured for the entire device.

You can configure one load-balancing mode for the entire device, a different mode for specified modules, and another mode for other specified modules. The per-module configuration takes precedence over the load-balancing configuration for the entire device.

Use the option that provides the balance criteria with the greatest variety in your configuration. For example, if the traffic on a port channel is going only to a single MAC address and you use the destination MAC address as the basis of port channel load balancing, the port channel always chooses the same link in that port channel; using source addresses or IP addresses might result in better load balancing.

This command does not require a license.

Examples

This example shows how to set the load-balancing method for the entire device to use the source port:

```
switch(config)# port-channel load-balance src-port
```

This example shows how to set the load-balancing method for the module level (for F2/F2e modules only).

```
switch(config)# port-channel load-balance vlan-only module 1
ERROR: Command is valid for F2/F2E Module only
switch(config)# port-channel load-balance vlan-only module 4
switch(config)#
```

Related Commands

Command	Description
<code>show port-channel load-balance</code>	Displays information about port-channel load balancing.

port-channel load-balance hash-modulo

To enable the modulo hash for Cisco nexus 7000 Series modules, use the **port-channel load-balance hash-modulo** command. To turn off this feature command, use the **no** form of this command.

port-channel load-balance hash-modulo force
no port-channel load-balance hash-modulo force

Syntax Description

force	Specifies the force.
--------------	----------------------

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
6.1(3)	This command was introduced.

Usage Guidelines



Caution

Once you enter the force keyword, the command immediately reinitializes all of the port channels.

By default, when the system comes if the system allows M1 Series Module capability and so, the port-channel load-balance hash-modulo displays an error. Enter the system module-type command to remove “M1 Series Module capability” first and then the command will work.

This command does not require a license.

Examples

This example shows how to enable the modulo hash for the Cisco nexus 7000 Series Module:

```
switch# port-channel load-balance hash-modulo
This command will reinitialize all the port-channels. Do you want to continue(y/n)? [no] y
Warning: This operation may take some time to complete
switch(config)#
```

This example shows how to specify the force:

```
switch# port-channel load-balance hash-modulo force
Warning: This operation may take some time to complete
```

This example shows how to turn on and off this feature:

```
switch(config)# no port-channel load-balance hash-modulo force
Warning: This operation may take some time to complete
switch(config)#
```

Related Commands

Command	Description
show port-channel load-balance	Displays information about port-channel load balancing.

port-channel load-defer

To set the load defer time interval, use the **port-channel load-defer** command. To return the system priority to the default value, use the **no** form of this command.

port-channel load-defer *seconds*
no port-channel load-defer *seconds*

Syntax Description	<i>seconds</i> Time interval in seconds. The range is from 1 to 1800.
---------------------------	---

Command Default 120 seconds

Command Modes Global configuration mode

Command History	Release	Modification
	5.1(2)	This command was introduced.

Examples

This example shows how to set the load defer time interval:

```
switch(config)# port-channel load-defer 100
switch(config)#
```

Related Commands	Command	Description
	show port-channel load-balance	Displays information about port-channel load balancing.

port-profile

To create a port profile and enter the port-profile configuration mode or to enter into the port-profile configuration mode of a previously created port profile, use the **port-profile** command. To remove the port profile, use the **no** form of this command.

port-profile [**type** {**ethernet** | **interface-vlan** | **port-channel**}] *name*
no port-profile [**type** {**ethernet** | **interface-vlan** | **port-channel**}] *name*

Syntax Description

type	(Optional) Specifies the type of interfaces.
ethernet	Specifies Layer 2 or Layer 3 interfaces.
interface-vlan	Specifies VLAN network interfaces.
port-channel	Specifies port-channel interfaces.
<i>name</i>	Name of the port profile.

Command Default

None

Command Modes

Interface configuration mode
 Port-profile configuration mode

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

Use the **port-profile** command to group configuration commands and apply them to several interfaces simultaneously. All interfaces in the range must be the same type. The maximum number of interfaces that can inherit a single port profile is 512.

The port-profile name must be globally unique across types and networks.

Each port profile can be applied only to a specific type of interface; the choices are as follows:

- Ethernet
- VLAN network interface
- Port channel



Note

When you choose **ethernet** as the interface type, the port profile is in the default mode which is Layer 3. Enter the **switchport** command to change the port profile to Layer 2 mode.

A subset of commands are available under the port-profile configuration mode, depending on which interface type you specify. Layer 3 and CTS commands are not supported by port profiles.

You can configure the following port-profile operations:

- Create port profiles
- Delete port profiles
- Add commands to and delete commands from port profiles
- Inherit port profiles at interfaces
- Enable and disable port profiles
- Inherit between port profiles
- Configure maximum number of ports that a profile can inherit

You inherit the port profile when you attach the port profile to an interface or range of interfaces. The maximum number of interfaces that can inherit a single profile is 512. When you attach, or inherit, a port profile to an interface or range of interfaces, the system applies all the commands in that port profile to the interfaces.

Additionally, you can have one port profile inherit another port profile, which allows the initial port profile to assume all of the commands of the second, inherited port profile that do not conflict with the initial port profile. Four levels of inheritance are supported except for the **switchport private-vlan mapping** and **private-vlan mapping** commands, which support only one level of inheritance. See the **inherit port-profile** command for information about inheriting an additional port profile and assigning port profiles to specified interfaces.

The system applies the commands inherited by the interface or range of interfaces according to the following guidelines:

- Commands that you enter under the interface mode take precedence over the port profile's commands if there is a conflict. However, the port profile retains that command in the port profile.
- The port profile's commands take precedence over default commands on the interface, unless it is explicitly overridden by the default command.
- When a range of interfaces inherits a second port profile, the commands of the initial port profile override those commands of the second port profile if there is a conflict.
- After you inherit a port profile onto an interface or range of interfaces, you can override individual configuration values by entering the new value at the interface configuration level. If you then remove the individual configuration values at the interface configuration level, the interface again uses the values in the port profile again.
- There are no default configurations associated with a port profile.



Note You cannot use port profiles with Session Manager.

If you delete a specific configuration for a specified range of interfaces using the interface configuration mode, that configuration is also deleted from the port profile for that range of interfaces only. For example, if you have a channel group inside a port profile and you are in the interface configuration mode and you delete that port channel, the specified port channel is also deleted from the port profile as well.

Just as in the device, you can enter a configuration for an object in port profiles without that object being applied to interfaces. For example, you can configure a VRF instance without it being applied to the system. If you then delete that VRF and its configurations from the port profile, the system is unaffected.

After you inherit a port profile on an interface or range of interfaces and you delete a specific configuration value, that port-profile configuration does not operate on the specified interfaces.

You must enable each specific port profile using the **state-enabled** command.

This command does not require a license.

Examples

This example shows how to configure, name a port profile, and enter the port-profile configuration mode:

```
switch(config)# port-profile type ethernet test
switch(config-ppm)#
```

Related Commands

Command	Description
state-enable	Enables a specified port profile.
show port-profile	Displays information about port profiles.

profile (EOAM)

To attach an Ethernet OAM profile to an interface, use the **profile** command in interface Ethernet OAM configuration mode. To remove the profile from the interface, use the **no** form of this command.

profile name
noprofile name

Syntax Description

name Text name of the Ethernet OAM profile to attach to the interface.

Command Default

None

Command Modes

Interface Ethernet OAM configuration (config-if-eoam)

Command History

Release	Modification
7.3(0)D1(1)	This command was introduced.

Usage Guidelines

When an Ethernet OAM profile is attached to an interface using this command, all of the parameters configured for the profile are applied to the interface.

Individual parameters that are set by the profile configuration can be overridden by configuring them directly on the interface.

This command does not require a license.

The following example shows how to attach an Ethernet OAM profile to a Ethernet interface.

```
switch# configure terminal
switch(config)# interface ethernet 2/19
switch(config-if)# ethernet oam
switch(config-if-eoam)# profile Profile_1
```

Related Commands

Command	Description
ethernet oam profile	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
show ethernet oam configuration	Displays the current active Ethernet OAM configuration on an interface.
show ethernet oam interfaces	Displays the current state of Ethernet OAM interfaces.



R Commands

- [rate-mode dedicated](#), on page 164
- [rate-mode shared](#), on page 166
- [reload restore](#), on page 167
- [remote-loopback disable](#), on page 168
- [role priority](#), on page 169
- [router ospfv3](#), on page 170

rate-mode dedicated

To set the dedicated rate mode for the specified ports, use the **rate-mode dedicated** command.

rate-mode dedicated
no rate-mode

Syntax Description This command has no arguments or keywords.

Command Default Shared rate mode is the default.

Command Modes Interface configuration mode

Command History	Release	Modification
	4.0	This command was introduced.

Usage Guidelines Use the rate-mode dedicated command to set the dedicated rate mode for the specified ports.

On a 32-port, 10-Gigabit Ethernet module, each set of four ports can handle 10 gigabits per second (Gb/s) of bandwidth. You can use the rate-mode parameter to dedicate that bandwidth to the first port in the set of four ports or share the bandwidth across all four ports.



Note When you dedicate the bandwidth to one port, you must first administratively shut down the ports in the group, change the rate mode to dedicated, and then bring the dedicated port administratively up.

[Table 3: Dedicated and Shared Ports, on page 164](#) identifies the ports that are grouped together to share each 10 Gb/s of bandwidth and which port in the group can be dedicated to utilize the entire bandwidth.

Table 3: Dedicated and Shared Ports

Ports Groups that Can Share Bandwidth	Ports that Can be Dedicated to Each 10-Gigabit Ethernet of Bandwidth
1, 3, 5, 7	1
2, 4, 6, 8	2
9, 11, 13, 15	9
10, 12, 14, 16	10
17, 19, 21, 23	17
18, 20, 22, 24	18
25, 27, 29, 31	25
26, 28, 30, 32	26



Note All ports in each port group must be part of the same virtual device context (VDC). For more information on VDCs, see the Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 5.x.

When you enter the **rate-mode dedicated** command, the full bandwidth of 10 Gbps is dedicated to one port. When you dedicate the bandwidth, all subsequent commands for the port are for dedicated mode.

This command does not require a license.

Examples

This example shows how to configure the dedicated rate mode for Ethernet ports 4/17, 4/19, 4/21, and 4/23:

```
switch# configure terminal
switch(config)# interface ethernet 4/17, ethernet 4/19, ethernet 4/21, ethernet 4/23
switch(config-if)# shutdown
switch(config-if)# interface ethernet 4/17
switch(config-if)# rate-mode dedicated
switch(config-if)# no shutdown
```

Related Commands

Command	Description
show interface	Displays interface information, which includes the current rate mode dedicated.

rate-mode shared

To set the shared rate mode for the specified ports, use the **rate-mode shared** command.

rate-mode shared

Syntax Description This command has no arguments or keywords.

Command Default Shared rate mode is the default.

Command Modes Interface configuration mode

Command History	Release	Modification
	4.0	This command was introduced.

Usage Guidelines Use the **rate-mode shared** command to set the shared rate mode for the specified ports. This is the default rate mode for the module.

That is, use the **rate-mode shared** command to specify that each 10 Gbps of bandwidth on a 32-port 10-Gigabit Ethernet module is shared by ports in the same port group.

If the port group is in dedicated rate mode, you must first administratively shut down the ports in the group, change the rate mode to shared, and then bring the ports administratively up.

This command does not require a license.

Examples

This example shows how to configure the shared rate mode for Ethernet ports 4/17, 4/19, 4/21, and 4/23:

```
switch# configure terminal
switch(config)# interface ethernet 4/17, ethernet 4/19, ethernet 4/21, ethernet 4/23
switch(config-if)# shutdown
switch(config-if)# interface ethernet 4/17
switch(config-if)# rate-mode shared
switch(config-if)# no shutdown
```

Related Commands

Command	Description
show interface	Displays interface information, which includes the current rate mode shared.

reload restore

To configure a virtual port channel (vPC) device to assume that its peer is not functional and to bring up the vPC, use the **reload restore** command. To reset the vPC to the standard behavior, use the **no** form of this command.

```
reload restore [delay time-out]
no reload restore
```

Syntax Description	delay <i>time-out</i>	(Optional) Sets the timeout for the vPC device. The range is from 240 to 3600.
---------------------------	---------------------------------	--

Command Default Delay of 240 seconds

Command Modes vPC domain configuration mode

Command History	Release	Modification
	5.2(1)	This command was deprecated.
	5.0(2)	This command was introduced.

Usage Guidelines This command does not require a license.

Examples

This example shows how to configure a vPC device to assume that its peer is not functional and to bring up the vPC:

```
switch(config)# vpc domain 5
switch(config-vpc-domain)# reload restore
Warning: Enables restoring of vPCs in a peer-detached state after reload, will wait for 240
sec (by default) to determine if peer is un-reachable
```

Related Commands	Command	Description
	vpc domain	Creates a virtual port-channel (vPC) domain.

remote-loopback disable

To perform no action on an interface when a remote-loopback event occurs, use the **remote-loopback disable** command in Ethernet OAM action configuration mode or interface Ethernet OAM action configuration mode. To remove the configuration, use the **no** form of this command.

remote-loopback {**disable** | **log**}
noremove-loopback {**disable** | **log**}

Syntax Description

disable	Performs no action on the interface when a remote-loopback event occurs.
log	(Interface Ethernet OAM action configuration only) Creates a syslog entry when a remoteloopback event occurs. This action is available in Interface Ethernet OAM action configuration mode to override the profile setting and log the event for the interface when it occurs.

Command Default

The default action is to create a syslog entry.

Command Modes

Ethernet OAM action configuration (config-eoam-action)
 Interface Ethernet OAM action configuration (config-if-eoam-action)

Command History

Release	Modification
7.3(0)D1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

The following example shows how to configure that no action is performed on the interface when a remote-loopback event occurs:

```
switch# configure terminal
switch(config)# ethernet oam profile Profile_1
switch(config-eoam)# action
switch(config-eoam-action)# remote-loopback disable
```

The following example shows how to configure that a syslog is created when a remote-loopback event occurs:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ethernet oam
switch(config-if-eoam)# action
switch(config-if-eoam-action)# remote-loopback log
```

Related Commands

Command	Description
ethernet oam profile	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM)	Attaches an Ethernet OAM profile to an interface.

role priority

To override the default selection of virtual port-channel (vPC) primary and secondary devices when you create a vPC domain, use the **role priority** command. To return to the default vPC system priority, use the **no** form of this command.

role priority *priority*
no role priority

Syntax Description	<i>priority</i> Role priority. The range is from 1 to 65636.
---------------------------	--

Command Default	32667
------------------------	-------

Command Modes	vpc-domain command mode
----------------------	-------------------------

Command History	Release	Modification
	4.1(3)	This command was introduced.

Usage Guidelines You must enable the vPC feature before you can create a vPC system priority

By default, the system elects a primary and secondary vPC peer device after you configure the vPC domain and both sides of the vPC peer link. However, you may want the system to elect a specific vPC peer device as the primary device for the vPC. Then, you would manually configure the role value for the vPC peer device that you want as primary to be lower than that of the other vPC peer device.

This command does not require a license.

Examples

This example shows how to create a vPC role priority:

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# role priority 2000
```

Related Commands	Command	Description
	show vpc role	Displays the role for this device for the vPC domain as primary or secondary.

router ospfv3

To configure Bidirectional Forwarding Detection (BFD) for the Open Shortest Path First version 3 (OSPFv3) routing process for all interfaces, use the **router ospfv3** command.

router ospfv3 *process-id*

Syntax Description

<i>process-id</i>	Configures an OSPFv3 routing process and that allows you to enter router configuration mode.
-------------------	--

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

OSPFv3 must be running on all participating devices. You must configure the baseline parameters for BFD sessions on the interfaces over which you want to run BFD sessions to discover BFD neighbors.

Examples

This example shows how to configure BFD for OSPFv3 for all interfaces:

```
switch# configure terminal
switch(config)# router ospfv3 3
switch(config-router)# bfd
switch(config-router)# exit
switch(config)#
```

Related Commands

Command	Description
show bfd	Displays the BFD commands.



S Commands

- [self-isolation](#), on page 172
- [session-down](#), on page 173
- [session-up](#), on page 175
- [shutdown](#), on page 176
- [shutdown lan](#), on page 177
- [speed](#), on page 178
- [state enabled](#), on page 180
- [switchport](#), on page 181
- [switchport access vlan](#), on page 182
- [switchport autostate exclude](#), on page 183
- [switchport dot1q ethertype](#), on page 184
- [switchport host](#), on page 185
- [switchport mode](#), on page 186
- [switchport mode dot1q-tunnel](#), on page 188
- [switchport trunk allowed vlan](#), on page 189
- [switchport trunk native vlan](#), on page 191
- [switchport trunk native vlan tag](#), on page 192
- [symbol-period threshold](#), on page 194
- [symbol-period window](#), on page 195
- [system-mac](#), on page 196
- [system-priority](#), on page 197
- [system default interface congestion mode](#), on page 198
- [system default interface congestion timeout](#), on page 199
- [system default interface pause mode](#), on page 201
- [system default interface pause timeout](#), on page 202
- [system default link-fail laser-on](#), on page 203
- [system default switchport](#), on page 204
- [system jumbomtu](#), on page 205
- [system module-type](#), on page 206

self-isolation

To enable virtual port-channel (vPC) self-isolation for the specified vPC domain, use the **self-isolation** command. To disable vPC self-isolation, use the **no** form of the command.

self-isolation
no self-isolation

Syntax Description This command has no arguments or keywords.

Command Default vPC self-isolation is disabled.

Command Modes vpc-domain command mode

Command History	Release	Modification
	7.1(1)D1(0)	This command was introduced.

Usage Guidelines Use the **self-isolation** command in vpc-domain command mode to enable the vPC self-isolation feature for the vPC domain.

The vPC self-isolation feature enables a vPC peer to self-isolate itself when a significant error is detected on the switch, thereby preventing the entire vPC complex being brought down.

This command does not require a license.

Examples This example shows how to enable vPC self-isolation:

```
switch(config)# vpc domain 1
switch(config-vpc-domain)# self-isolation
```

Related Commands	Command	Description
	show vpc brief	Displays information about vPCs.
	show vpc statistics	Displays vPC statistics.
	vpc domain	Configures a vPC domain and enters the vpc-domain configuration mode.

session-down

To configure what action is taken on an interface when an Ethernet OAM session goes down, use the **session-down** command in Ethernet OAM action configuration mode or interface Ethernet OAM action configuration mode. To remove the configuration, use the **no** form of this command.

```
session-down {disable | efd | error-disable-interface | log}
nosession-down {disable | efd | error-disable-interface | log}
```

Syntax Description	disable	Performs no action on the interface when an Ethernet OAM session goes down.
	efd	Puts the line protocol into the down state for an interface when an Ethernet OAM session goes down.
	error-disable-interface	Puts the interface into the error-disable state when an Ethernet OAM session goes down.
	log	(Interface Ethernet OAM action configuration only) Creates a syslog entry when an Ethernet OAM session goes down. This action is available in Interface Ethernet OAM action configuration mode to override the profile setting and log the event for the interface when it occurs.

Command Default The default action is to create a syslog entry.

Command Modes Ethernet OAM action configuration (config-eoam-action)
Interface Ethernet OAM action configuration (config-if-eoam-action)

Command History	Release	Modification
	7.3(0)D1(1)	This command was introduced.

Usage Guidelines This command does not require a license.

The following example shows how to configure that no action is performed on the interface when an Ethernet OAM session goes down:

```
switch# configure terminal
switch(config)# ethernet oam profile Profile_1
switch(config-eoam)# action
switch(config-eoam-action)# session-down disable
```

The following example shows how to configure putting the interface into the line-protocol-down state when an Ethernet OAM session goes down:

```
switch# configure terminal
switch(config)# ethernet oam profile Profile_1
switch(config-eoam)# action
switch(config-eoam-action)# session-down efd
```

The following example shows how to configure that the interface is put into the error-disable state when an Ethernet OAM session goes down:

```

switch# configure terminal
switch(config)# ethernet oam profile Profile_1
switch(config-eoam)# action
switch(config-eoam-action)# session-down error-disable-interface

```

The following example shows how to configure that a syslog is created when an Ethernet OAM session goes down:

```

switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ethernet oam
switch(config-if-eoam)# action
switch(config-if-eoam-action)# session-down log

```

Related Commands

Command	Description
ethernet oam profile	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM)	Attaches an Ethernet OAM profile to an interface.

session-up

To perform no action on an interface when an Ethernet OAM session is established, use the **session-up disable** command in Ethernet OAM action configuration mode or interface Ethernet OAM action configuration mode. To remove the configuration, use the **no** form of this command.

```
session-up {disable | log}
nosession-up {disable | log}
```

Syntax Description	disable	Performs no action on the interface when an Ethernet OAM session is established.
	log	(Interface Ethernet OAM action configuration only) Creates a syslog entry when an Ethernet OAM session is established. This action is available in Interface Ethernet OAM action configuration mode to override the profile setting and log the event for the interface when it occurs.

Command Default The default action is to create a syslog entry.

Command Modes Ethernet OAM action configuration (config-eoam-action)
Interface Ethernet OAM action configuration (config-if-eoam-action)

Command History	Release	Modification
	7.3(0)D1(1)	This command was introduced.

Usage Guidelines This command does not require a license.

The following example shows how to configure that no action is performed on the interface when an Ethernet OAM session is established:

```
switch# configure terminal
switch(config)# ethernet oam profile Profile_1
switch(config-eoam)# action
switch(config-eoam-action)# session-up disable
```

The following example shows how to configure that a syslog is created when an Ethernet OAM session is established:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ethernet oam
switch(config-if-eoam)# action
switch(config-if-eoam-action)# session-up log
```

Related Commands

Command	Description
ethernet oam profile	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM)	Attaches an Ethernet OAM profile to an interface.

shutdown

To bring the port administratively down, use the **shutdown** command. To bring the port administratively up, use the **no shutdown** command.

shutdown [**force**]
no shutdown [**force**]

Syntax Description

force	(Optional) Forces the interface state to change. When you shut down a management interface, a warning question is displayed regarding active Telnet sessions. You can bypass the question with the force option. The force option is also useful when you run an automated configuration playback. The force option is only available for Ethernet interfaces or the management port.
--------------	--

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the shutdown command to bring the port administratively down. Use the **no shutdown** command to bring the port administratively up.

This command does not require a license.

Examples

This example shows how to bring the port administratively down:

```
switch(config-if)# shutdown
```

This example shows how to bring the port administratively up:

```
switch(config-if)# no shutdown
```

Related Commands

Command	Description
interface ethernet	Configures the types and identities of Ethernet interfaces.

shutdown lan

To shut down LAN VLANs on a shared Ethernet interface, use the **shutdown lan** command. To bring up the LAN VLAN on a shared Ethernet interface, use the **no shutdown lan** command.

shutdown lan
no shutdown lan

Syntax Description This command has no keywords or arguments.

Command Default Disabled

Command Modes Interface configuration mode

Command History	Release	Modification
	6.2(6)	This command was introduced.

Usage Guidelines Use the **shutdown lan** command to enable you to shut down the LAN VLANs on a shared Ethernet interface. The **no** form of this command brings up the LAN VLAN on a shared Ethernet interface.



Note The **shutdown lan** command is supported on shared interfaces only.

The Link Layer Discovery Protocol (LLDP) must be enabled in the Ethernet VDC for shutdown LAN. This command does not require a license.

Examples

This example shows how to shut down Ethernet traffic on the interface:

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# shutdown lan
```

Related Commands	Command	Description
	interface ethernet	Configures the types and identities of Ethernet interfaces.

speed

To set the speed for Ethernet ports or management interfaces or set the port to autonegotiate its speed with other ports on the link, use the **speed** command.

speed {**10** | **100** | **1000** | **10000** | **auto** [**10** [**100** [**1000**]]]}

Syntax Description

10	Sets the speed at 10 Mbps.
100	Sets the speed at 100 Mbps.
1000	Sets the speed at 1 Gbps.
10000	Sets the speed at 10 Gbps.
auto	Sets the interface to autonegotiation.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Before you begin, make sure that the remote port has a speed setting that supports your changes for the local port. If you want to set the local port to use a specific speed, you must set the remote port for the same speed or set the local port to autonegotiate the speed.

The interface speed and duplex mode are interrelated, so you should configure both of their parameters at the same time.

The interface speed that you specify can affect the duplex mode used for an interface, so you should set the speed before setting the duplex mode. If you set the speed for autonegotiation, the duplex mode is automatically set to be autonegotiated. If you specify 10- or 100-Mbps speed, the port is automatically configured to use half-duplex mode, but you can specify full-duplex mode instead. If you specify a speed of 1000 Mbps (1 Gbps) or faster, full duplex is automatically used. For more details about configuring this command, see the *Cisco NX-OS Interfaces Configuration Guide* .

This command does not require a license.

Examples

This example shows how to set the speed of Ethernet port 1 on the 48-port 10/100/1000 module in slot 3 to 1000 Mbps and full-duplex mode:

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# speed 1000
switch(config-if)# duplex full
```

Related Commands

Command	Description
duplex	Specifies the duplex mode as full, half, or autonegotiate.
show interface	Displays the interface status, which includes the speed parameters.

state enabled

To enable the specified port profile, use the **state enabled** command. To return to the default value, use the **no** form of this command.

state enabled
no state enabled

Syntax Description This command has no keywords or arguments.

Command Default Disabled

Command Modes Port-profile configuration mode

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines Use the **state enabled** command to enable the specified port profile. See the **port-profile** command for information about the port-profile feature.

To apply the port-profile configurations to the interfaces, you must enable the specific port profile. You can configure and inherit a port profile onto a range of interfaces prior to enabling the port profile; you would then enable that port profile for the configurations to take effect on the specified interfaces. The maximum number of interfaces that can inherit a single profile is 512.

If you inherit one or more port profiles onto an original port profile, only the last inherited port profile must be enabled; the system assumes that the underlying port profiles are enabled.

This command does not require a license.

Examples

This example shows how to enable the port-profile feature:

```
switch(config)# port-profile type ethernet test
switch(config-ppm)# state enabled
```

Command	Description
show port-profile	Displays information about the port profiles.

switchport

To set the interface as a Layer 2 switching port, use the **switchport** command. To return the interface to the default Layer 3 routed interface status and cause all Layer 2 configuration to be erased, use the **no** form of this command.

switchport
no switchport

Syntax Description This command has no keywords or arguments.

Command Default Interfaces are Layer 3 by default.

Command Modes Interface configuration mode

Command History	Release	Modification
	4.0	This command was introduced.

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 additional **switchport** commands with keywords. This action is required only if you have not entered the **switchport** command for the interface.

The default switchport mode is the access mode. Use the **switchport mode** command to do the following:

- Set the interface to the Layer 2 access mode
- Return the interface to the Layer 2 trunk mode
- Use the interface with private VLANs

Enter the **no switchport** command to shut down the port and then reenables it. This action may generate messages on the device to which the port is connected.

When you use the **no switchport** command, all the Layer 2 configuration is deleted from that interface, and the interface has the default VLAN configuration.

The port goes down and reinitializes when you change the interface mode.

This command does not require a license.

Examples

This example shows how to cause a port interface to stop operating as a Cisco routed port and convert to a Layer 2 switched interface:

```
switch(config-if) # switchport
```

Related Commands	Command	Description
	show interface switchport	Displays the administrative and operational status of a switching (nonrouting) port.

switchport access vlan

To set the access VLAN when the interface is in access mode, use the **switchport access vlan** command. 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

<i>vlan-id</i>	VLAN to set when the interface is in access mode; valid values are from 1 to 4094, except for the VLANs reserved for internal switch use.
----------------	---

Command Default

VLAN1

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0	This command was introduced.

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.

Enter the **no switchport access vlan** command to shut down the port and then reenab it. This action may generate messages on the device to which the port is connected.

Use the no form of the **switchport access vlan** command to reset the access-mode VLAN to the appropriate default VLAN for the device.

This command does not require a license.

Examples

This example shows how to cause a port interface that has already been configured as a switched interface to operate as an access port in VLAN 2 instead of the platform's default VLAN in the interface-configuration mode:

```
switch(config-if)# switchport access vlan 2
```

Related Commands

Command	Description
show interface switchport	Displays the administrative and operational status of a switching (nonrouting) port.

switchport autostate exclude

To exclude an access port or trunk from the VLAN interface link-up calculation on the Cisco NX-OS device, use the `switchport autostate exclude` command. To revert 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
	5.0	This command was introduced.

Usage Guidelines

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 **show interface 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.

This command does not require a license.

Examples

This example shows how to exclude a port from the VLAN interface link-up calculation on the Cisco NX-OS device:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# switchport
switch(config-if)# switchport autostate exclude
```

This example shows how to include all ports in the VLAN interface link-up calculation on the Cisco NX-OS device:

```
switch(config-if)# no switchport autostate exclude
```

Related Commands	Command	Description
	switchport	Configures the interface as a Layer 2 switching port.
	show interface switchport	Displays the administrative and operational status of a switching (nonrouting) port.

switchport dot1q ethertype

To set the EtherType used for Q-in-Q encapsulation on an interface, use the **switchport dot1q ethertype** command. To reset the EtherType to its default value, Use the **no** form of this command.

switchport dot1q ethertype *ethertype*
no switchport dot1q ethertype [*ethertype*]

Syntax Description

<i>ethertype</i>	Value to set for the EtherType. The range is from 0x600 to 0xffff. <ul style="list-style-type: none"> • 0x8100 is the default EtherType for 802.1q frames • 0x88A8 is the EtherType for 802.1ad double tagged frames • 0x9100 is the EtherType for QinQ frames
------------------	---

Command Default

0x8100 is the default EtherType for 802.1q frames

Command Modes

Interface configuration mode

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

You must enter the **switchport** command without any keywords to configure the Ethernet interface as a Layer 2 interface before you can enter the **switchport mode** command. This action is required only if you have not entered the **switchport** command for the interface.

You must set the EtherType only on the egress trunk interface that carries double tagged frames (the trunk interface that connects the service providers). If you change the EtherType on one side of the trunk, you must set the same value on the other end of the trunk (symmetrical configuration).



Caution

The EtherType value you set affects all the tagged packets going out on the interface (not just Q-in-Q packets).

This command does not require a license.

Examples

This example shows how to create a 802.1Q tunnel on an interface:

```
switch(config-if)# switchport dot1q ethertype 0x9100
```

Related Commands

Command	Description
show interface switchport	Displays information about all the switch port interfaces.

switchport host

To configure a port that is not connected to any other devices as a Layer 2 access port with optimized packet forwarding, use the **switchport host** command. To disable a port that is not connected to any other devices as a Layer 2 access, use the **no** form of this command.

switchport host
no switchport host

Syntax Description This command has no keywords or arguments.

Command Default Interfaces are Layer 3 by default.

Command Modes Interface configuration mode

Command History	Release	Modification
	4.0	This command was introduced.

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 host** command. This action is required only if you have not entered the **switchport** command for the interface.

Entering the **switchport host** command on an interface:

- Makes the Layer 2 interface an access port.
- Makes the Layer 2 interface an STP edge port, which decreases the time that it takes to start up packet forwarding.
- Disables port channeling on this interface.

You should enter the **switchport host** command only on ports that are connected to a single host. When you use this command with an interface connected to other than a single host, the device returns an error message.

To optimize the port configuration, entering the **switchport host** command sets the switch port mode to access and disables channel grouping. Only an end station can accept this configuration.

This command toggles the port if it is in the UP state.

This command does not require a license.

Examples

This example shows how to optimize an access port configuration for a host connection:

```
switch(config-if)# switchport host
```

Related Commands	Command	Description
	show interface switchport	Displays the administrative and operational status of a switching (nonrouting) port.

switchport mode

To set the Layer 2 interface type, use the **switchport mode** command. To return the interface to the Layer 2 access mode, use the **no** form of this command.

```
switchport mode {access | dot1q-tunnel | fabricpath | fex-fabric | private-vlan {host | promiscuous |
trunk [{promiscuous | secondary}]} | trunk}
no switchport mode
```

Syntax Description

access	Specifies the interface as a nontrunking, nontagged single-VLAN Layer 2 interface. An access port carries traffic in one VLAN only.
dot1q-tunnel	Creates a 802.1Q tunnel on the interface.
fabricpath	Specifies the port mode as FabricPath.
fex-fabric	Sets the interface type to be an uplink port for a Fabric Extender.
private-vlan	Sets the port mode as a private-VLAN (PVLAN) host.
host	Sets the port mode as the PVLAN host.
promiscuous	(Optional) Sets the port mode as PVLAN promiscuous.
secondary	(Optional) Sets the port mode trunk as isolated.
trunk	Specifies the trunking VLAN interface in Layer 2. A trunk port can carry traffic in one or more VLANs (based on the trunk allowed VLAN list configuration) on the same physical link.

Command Default

access ports

Command Modes

Interface configuration mode

Command History

Release	Modification
5.2(1)	Added the dot1q-tunnel, fabricpath, fex-fabric, private-vlan, host, promiscuous, and secondary keywords.
4.0	This command was introduced.

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 mode** command. This action is required only if you have not entered the **switchport** command for the interface.

If you enter **access** mode, the interface goes into nontrunking mode; if you enter **trunk** mode, the interface goes into trunking mode.

To correctly deliver the traffic on a trunk port with several VLANs, the switch uses the IEEE 802.1Q encapsulation, or tagging, method. If an access port receives a packet with an 802.1Q tag in the header, that port drops the packet without learning its MAC source address.



Note A port can function as either an access port, a trunk port, or a private VLAN port; a port cannot function as all three simultaneously.

The port goes down and reinitializes when you change the interface mode.

This command does not require a license.

Examples

This example shows how to set the interface to trunking mode:

```
switch(config-if) # switchport mode trunk
```

Related Commands

Command	Description
show interface switchport	Displays the administrative and operational status of a switching (nonrouting) port.

switchport mode dot1q-tunnel

To create an 802.1Q tunnel on an interface, use the **switchport mode dot1q-tunnel** command. To disable the 802.1Q tunnel on the interface, use the **no** form of this command.

switchport mode dot1q-tunnel
no switchport mode dot1q-tunnel

Syntax Description This command has no arguments or keywords.

Command Default No 802.1Q tunnel

Command Modes Interface configuration mode

Command History	Release	Modification
	5.0(2)	This command was introduced.

Usage Guidelines You must enter the **switchport** command without any keywords to configure the Ethernet interface as a Layer 2 interface before you can enter the **switchport mode** command. This action is required only if you have not entered the **switchport** command for the interface.

The port goes down and reinitializes (port flap) when the interface mode is changed. BPDU filtering is enabled and the Cisco Discovery Protocol (CDP) is disabled on tunnel interfaces.

This command does not require a license.

Examples

This example shows how to create a 802.1Q tunnel on an interface:

```
switch(config-if)# switchport mode dot1q-tunnel
```

Related Commands	Command	Description
	switchport mode fex-fabric	Sets the interface type to be an uplink port for a Fabric Extender.

switchport trunk allowed vlan

To set the list of allowed VLANs on the trunking interface, use the **switchport trunk allowed vlan** command. To allow all VLANs on the trunking interface, use the **no** form of this command.

switchport trunk allowed vlan {*vlan-list* | **add** *vlan-list* | **all** | **except** *vlan-list* | **none** | **remove** *vlan-list*}
no switchport trunk allowed vlan

Syntax Description	
<i>vlan-list</i>	Allowed VLANs that transmit through this interface in tagged format when in trunking mode; the range of valid values is from 1 to 4094.
add	Adds the defined list of VLANs to those currently set instead of replacing the list.
all	Allows all appropriate VLANs to transmit through this interface in tagged format when in trunking mode.
except	Allows all VLANs to transmit through this interface in tagged format when in trunking mode except the specified values.
none	Blocks all VLANs transmitting through this interface in tagged format when in trunking mode.
remove	Removes the defined list of VLANs from those currently set instead of replacing the list.

Command Default All VLANs

Command Modes Interface configuration mode

Command History	Release	Modification
	4.0	This command was introduced.

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 trunk allowed vlan** command. This action is required only if you have not entered the **switchport** command for the interface.

You can enter the **switchport trunk allowed vlan** command on interfaces where the Switched Port Analyzer (SPAN) destination port is either a trunk or an access port.

If you remove VLAN 1 from a trunk, the trunk interface continues to send and receive management traffic in VLAN 1.



Note The **switchport trunk allowed vlan** command is not supported on FEX fabric interfaces.

This command does not require a license.

Examples

This example shows how to add a series of consecutive VLANs to the list of allowed VLANs on a trunking port:

```
switch(config-if)# switchport trunk allowed vlan add 40-50
```

Related Commands

Command	Description
show interface switchport	Displays the administrative and operational status of a switching (nonrouting) port.

switchport trunk native vlan

To change the native VLAN ID when the interface is in trunking mode, use the **switchport trunk native vlan** command. To return the native VLAN ID to VLAN 1, use the **no** form of this command.

switchport trunk native vlan *vlan-id*
no switchport trunk native vlan

Syntax Description

<i>vlan-id</i>	Native VLAN for the trunk in 802.1Q trunking mode. The range is from 1 to 4094, except the internally reserved VLANs are 3968 to 4047 and 4094.
----------------	---

Command Default

VLAN1

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0	This command was introduced.

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 trunk native vlan** command. This action is required only if you have not entered the **switchport** command for the interface.

Changing the native VLAN on an access port or trunk port will flap the interface. This behavior is expected.



Note

See the **vlandot1q tag native** command for more information about configuring the native VLAN for 802.1Q trunk ports.

Use the **no** form of the **native vlan** command to reset the native mode VLAN to the default VLAN1 for the device.

This command does not require a license.

Examples

This example shows how to configure the native VLAN for an interface in trunk mode:

```
switch(config-if)# switchport trunk native vlan 5
```

Related Commands

Command	Description
show interface switchport	Displays the administrative and operational status of a switching (nonrouting) port.

switchport trunk native vlan tag

To enable native VLAN tagging on a trunk port, use the **switchport trunk native vlan tag** command. To remove native VLAN tagging on a trunk port, use the **no** form of this command.

switchport trunk native vlan tag [exclude control]
no switchport trunk native vlan tag [exclude control]

Syntax Description	exclude control	(Optional) Excludes untagged control packets on the native VLAN.
---------------------------	------------------------	--

Command Default **Packets (both control and data) are untagged on the native VLAN.**

Command Modes Interface configuration mode

Command History	Release	Modification
	6.2(10)	This command was introduced.

Usage Guidelines The **switchport trunk native vlan tag** command is applicable only for trunk ports.

For trunk ports, the default behavior is that packets (both control and data) are untagged. The **switchport trunk native vlan tag** command allows you to tag or untag control and data packets of the native VLAN. The tagging states are:

- **switchport trunk native vlan tag**—Both control and data packets of the native VLAN are tagged.
- **switchport trunk native vlan tag exclude control**—Data packets are tagged and control packets are untagged.
- **no switchport trunk native vlan tag** and **no switchport trunk native vlan tag exclude control**—Both control and data packets are untagged

When a port-level configuration is applied, the global configuration for native VLAN tagging will no longer take effect on that port. Port-level configurations take priority over global configurations.

This command does not require a license.

Examples

This example shows how to configure the native VLAN for an interface in trunk mode:

```
switch(config)# interface ethernet7/1
switch(config-if)# switchport
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk native vlan tag
```

Related Commands	Command	Description
	show vlan dot1q tag native	Displays native VLAN-tagging information.
	switchport	Specifies the interface as a Layer 2 switching port.

Command	Description
switchport mode	Specifies the Layer 2 interface type.

symbol-period threshold

To configure the thresholds that trigger an Ethernet OAM symbol-period error event, use the **symbol-period threshold** command in Ethernet OAM link monitor configuration mode. To remove the configuration, use the **no** form of this command.

```
symbol-period threshold low threshold [high threshold]  
no symbol-period threshold [low threshold [high threshold]]
```

Syntax Description	<p>low<i>threshold</i> Low threshold value, in symbols, that triggers a symbol-period error event. The range is 1 to 60000000.</p> <p>high<i>threshold</i> (Optional) High threshold value, in symbols, that triggers a symbol-period error event. The range is 1 to 60000000. The high threshold value can be configured only in conjunction with the low threshold value.</p>				
Command Default	The default low threshold value is 1. There is no default high threshold value.				
Command Modes	Ethernet OAM link monitor configuration (config-eoam-lm) Interface Ethernet OAM link monitor configuration (config-if-eoam-lm)				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>7.3(0)D1(1)</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	7.3(0)D1(1)	This command was introduced.
Release	Modification				
7.3(0)D1(1)	This command was introduced.				

Usage Guidelines

When the low threshold is passed, a symbol-period error event notification is generated and transmitted to the OAM peer. Additionally, any registered higher level OAM protocols, such as Connectivity Fault Management (CFM), are also notified. When the high threshold is passed, the configured high threshold action is performed in addition to the low threshold actions. The high threshold is optional and is configurable only in conjunction with the low threshold.

This command does not require a license.

The following example shows how to configure the symbol-period low and high thresholds that trigger a symbol-period error event:

```
switch(config)# ethernet oam profile Profile_1  
switch(config-eoam)# link-monitor  
switch(config-eoam-lm)# symbol-period threshold low 100 high 6000
```

symbol-period window

To configure the window size for an Ethernet OAM symbol-period error event, use the **symbol-period window** command in Ethernet OAM link monitor or interface Ethernet OAM link monitor configuration mode. To remove the configuration, use the **no** form of this command.

symbol-period window *window*
nosymbol-period window *window*

Syntax Description	<i>window</i> Size of the window for symbol-period error in milliseconds. The range is 1000 to 60000.				
Command Default	The default window size value is 1000.				
Command Modes	Ethernet OAM link monitor configuration (config-eoam-lm) Interface Ethernet OAM link monitor configuration (config-if-eoam-lm)				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>7.3(0)D1(1)</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	7.3(0)D1(1)	This command was introduced.
Release	Modification				
7.3(0)D1(1)	This command was introduced.				
Usage Guidelines	<p>This command does not require a license.</p> <p>The following example shows how to configure the window size for a symbol-period error.</p> <pre>switch(config)# ethernet oam profile Profile_1 switch(config-eoam)# link-monitor switch(config-eoam-lm)# symbol-period window 60000</pre>				

system-mac

To overwrite the MAC address that the device creates for the virtual port-channel (vPC) domain when you create a vPC domain, use the **system-mac** command. To return to the default vPC system MAC address, use the **no** form of this command.

```
system-mac mac-address
no system-mac
```

Syntax Description	<i>mac-address</i> MAC address that you want for the vPC domain using the format xxxx.xxxx.xxxx.				
Command Default	None				
Command Default	vpc-domain command mode				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>4.1(3)</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	4.1(3)	This command was introduced.
Release	Modification				
4.1(3)	This command was introduced.				

Usage Guidelines You must enable the vPC feature before you can create a vPC system MAC address.

Use the **system-mac** command to overwrite the MAC address created by the system once you create a vPC domain. By default, the system creates a MAC address for the vPC when you create a vPC domain based on the domain ID. Cisco reserved a range of MAC addresses from the IEEE for this purpose and these addresses are used to complete the last 10 bits of the vPC domain MAC address. The range of default MAC addresses is as follows:

- Number of reserved MAC addresses—1024
- Starting—002304eebe00
- Ending—002304eec1ff

This command does not require a license.

Examples

This example shows how to create a vPC system MAC address:

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# system-mac 22cd.34ab.ca32
```

Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>show vpc role</td> <td>Displays the system MAC address for the vPC domain.</td> </tr> </tbody> </table>	Command	Description	show vpc role	Displays the system MAC address for the vPC domain.
Command	Description				
show vpc role	Displays the system MAC address for the vPC domain.				

system-priority

To overwrite the system priority that the device creates for the virtual port-channel (vPC) domain when you create a vPC domain, use the **system-priority** command. To return to the default vPC system priority, use the **no** form of this command.

system-priority *priority*
no system-priority *priority*

Syntax Description	<i>priority</i> System priority. The range is from 1 to 65535.
---------------------------	--

Command Default	32667
------------------------	-------

Command Modes	vpc-domain command mode
----------------------	-------------------------

Command History	Release	Modification
	4.1(3)	This command was introduced.

Usage Guidelines You must enable the vPC feature before you can create a vPC system priority.



Note We recommend that you manually configure the vPC system priority when you are running LACP to ensure that the vPC peer devices are the primary devices on LACP.

This command does not require a license.

Examples

This example shows how to create a vPC system priority:

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# system-priority 4000
```

Related Commands	Command	Description
	show vpc role	Displays the system priority for the vPC domain.

system default interface congestion mode

To configure the default interface congestion mode, use the system default interface congestion mode command. To disable this feature, use the **no** form of this command.

```
system default interface congestion mode {core | edge}
no system default interface congestion mode {core | edge}
```

Syntax Description

core	Specifies the core port type.
edge	Specifies the edge port type.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.1(1)	This command was introduced.

Usage Guidelines

None

Examples

This example shows how to configure the default interface congestion mode for the core port type:

```
switch# configure terminal
switch(config)# system default interface congestion mode core
switch(config)#
```

This example shows how to disable the default interface congestion mode for the edge port type:

```
switch# configure terminal
switch(config)# no system default interface congestion mode edge
switch(config)#
```

Related Commands

Command	Description
show system default switchport	Displays default values for switch port attributes.
show interface brief	Displays FC port modes.

system default interface congestion timeout

To configure the default value for a congestion timeout, use the system default interface congestion timeout command. To disable this feature, use the **no** form of this command.



Note Beginning from Cisco NX-OS Release 8.2(1), use the **system timeout fcoe congestion-drop** *{milliseconds}* **{default}** **mode** **{core | edge}** command to configure congestion timeout for slow drain.

```
system default interface congestion timeout milliseconds mode {core | edge}
no system default interface congestion timeout milliseconds mode {core | edge}
```

Syntax Description

<i>milliseconds</i>	Number of milliseconds. The range is from 100 to 1000 milliseconds.
mode	Specifies the mode.
core	Specifies the core port type.
edge	Specifies the edge port type.

Command Default

500 milliseconds

Command Modes

Global configuration mode

Command History

Release	Modification
6.1(1)	This command was introduced.

Usage Guidelines

Setting a smaller timeout on the edge ports such as 100 or 200 milliseconds helps to reduce the congestion on the edge port by making the packets on that port timeout sooner when they see the pause condition.



Note You should use the default configuration for core ports and a value that does not exceed 500 ms (100 to 200 ms preferable) for fabric edge ports.

Examples

This example shows how to configure the default value for a congestion timeout for the core type:

```
switch# configure terminal
switch(config)# system default interface congestion timeout 100 mode core
switch(config)#
```

This example shows how to disable the default value for a congestion timeout for the edge type:

```
switch# configure terminal
switch(config)# no system default interface congestion timeout 100 mode edge
switch(config)#
```

Related Commands

Command	Description
show system default switchport	Displays default values for switch port attributes.
show interface brief	Displays FC port modes.

system default interface pause mode

To configure the default timeout value for a pause frame, use the system default interface pause mode command. To disable this feature, use the **no** form of this command.

```
system default interface pause mode {core | edge}
no system default interface pause mode {core | edge}
```

Syntax Description

core	Specifies the core port type.
edge	Specifies the edge port type.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.1(1)	This command was introduced.

Usage Guidelines

None

Examples

This example shows how to configure the default timeout value for a pause frame for the core port type:

```
switch# configure terminal
switch(config)# system default interface pause mode core
switch(config)#
```

This example shows how to disable the timeout default value for a pause frame for the edge port type:

```
switch# configure terminal
switch(config)# no system default interface pause mode edge
switch(config)#
```

Related Commands

Command	Description
show system default switchport	Displays default values for switch port attributes.
show interface brief	Displays FC port modes.

system default interface pause timeout

To configure the default timeout value for a pause frame, use the system default interface pause timeout command. To disable this feature, use the **no** form of this command.

```
system default interface pause timeout milliseconds mode {core | edge}
no system default interface pause timeout milliseconds mode {core | edge}
```

Syntax Description

milliseconds	Number of milliseconds. The range is from 100 to 500 milliseconds.
mode	Specifies the mode.
core	Specifies the port type.
edge	Specifies the edge port type.

Command Default

500 milliseconds

Command Modes

Global configuration mode

Command History

Release	Modification
6.1(1)	This command was introduced.

Usage Guidelines

When the port is in the PAUSE state for the configured period, pause frame timeout can be enabled on that port, which results in all frames that come to that port getting dropped in the egress. This action frees up the buffer space in the ISL link (which carries traffic for this port) and helps to reduce congestion on other unrelated flows, use the same link.

Examples

This example shows how to configure the timeout value pause frame for the core port type:

```
switch# config terminal
switch(config)# system default interface pause timeout 100 mode core
switch(config)#
```

This example shows how to disable the timeout value pause for the edge port type:

```
switch# config terminal
switch(config)# no system default interface pause timeout 100 mode edge
switch(config)#
```

Related Commands

Command	Description
show system default switchport	Displays default values for switch port attributes.
show interface brief	Displays FC port modes.

system default link-fail laser-on

To prevent the laser from turning off when a link failure occurs, use the **system default link-fail laser-on** command. To return to the default setting, use the **no** form of this command.

```
system default link-fail laser-on
no system default link-fail laser-on
```

Command Default See the Usage Guidelines section.

Command Modes Global configuration mode

Command History

Release	Modification
6.2(12)	This command was introduced.

Usage Guidelines When a link failure is detected, the default behavior is for the laser to turn off for a few microseconds. This command overrides the default behavior and prevents the laser from turning off when there is a link failure.



Note Only F3 line cards support this feature.

Examples

This example shows how to prevent the laser from turning off when a link failure occurs:

```
switch# configure terminal
switch(config)# system default link-fail laser-on
```

This example shows how to return to the default behavior (where the laser turns off when a link failure occurs):

```
switch# configure terminal
switch(config)# no system default link-fail laser-on
```

system default switchport

To change the default interface mode for the system from Layer 3 routing to Layer 2 switching, use the **system default switchport** command. To return the system to Layer 3 routing default interface mode, use the **no** form of this command.

```
system default switchport [{fabricpath | shutdown}]
no system default switchport [{fabricpath | shutdown}]
```

Syntax Description	Parameter	Description
	fabricpath	(Optional) Configures the default port mode as FabricPath.
	shutdown	(Optional) Configures the administrative state as down.

Command Default None

Command Modes Global configuration mode

Command History	Release	Modification
	5.2(1)	Added the fabricpath keyword.
	4.0	This command was introduced.

Usage Guidelines The **system default switchport** command makes all the interfaces Layer 2 access ports. This command does not require a license.

Examples This example shows how to configure the system so that all the interfaces are in Layer 2 access mode:

```
switch(config-if)#
 system default switchport
```

Related Commands	Command	Description
	show interface switchport	Displays the administrative and operational status of a switching (nonrouting) port.

system jumbomtu

To configure the system jumbo maximum transmission unit (MTU) size for Layer 2 interfaces, use the **system jumbomtu** command.

system jumbomtu *size*

Syntax Description

<i>size</i>	Even number between 1500 and 9216.
-------------	------------------------------------

Command Default

The system jumbo MTU default size is 9216 bytes and the interface default MTU is 1500 bytes.

Command Modes

Global configuration mode

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **system jumbomtu** command to specify the MTU size for Layer 2 interfaces. The range is from 1500 to 9216.

The physical level uses an unchangeable bandwidth of 1 GB.

This command does not require a license.

Examples

This example shows how to configure the system jumbo MTU as 8000 bytes and how to change the MTU specification for an interface that was configured with the previous jumbo MTU size:

```
switch# configure terminal
switch(config)# system jumbomtu 8000
switch(config)# show running-config
switch(config)# interface ethernet 2/2
switch(config-if)# switchport
switch(config-if)# mtu 4608
```

Related Commands

Command	Description
show running-config	Displays the current operating configuration, which includes the system jumbo MTU size .

system module-type

To control which type of modules are allowed in this chassis, use the **system module-type** command. To return to the default settings, use the **no** form of this command.

system module-type *module-type*
no system module-type *module-type*

Syntax Description

<i>module-type</i>	f1 — Enables f1 type modules in the chassis. f2—Enables f2 type modules in the chassis. m1—Enables m1 type modules in the chassis. m1x1—Enables m1x1 type modules in the chassis. m2x1—Enables m2x2 type modules in the chassis.
--------------------	--

Command Default

None

Command Modes

Global configuration mode.

Command History

Release	Modification
6.1(3)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to control the type of modules that are allowed in this chassis:

```
switch# configure terminal
switch(config)# system module-type f1 m1x1 f2 m2x1 fc f2e
Modules of unsupported types will not be allowed to power on after this. Continue(y/n)?
[yes]
switch(config)#
```

Related Commands

Command	Description
show vpc role	Displays the system MAC address for the vPC domain.



Show Commands

- [show bfd neighbors](#), on page 209
- [show cfs application](#), on page 213
- [show errdisable](#), on page 215
- [show ethernet oam configuration](#), on page 217
- [show ethernet oam discovery](#), on page 219
- [show ethernet oam event-log](#), on page 221
- [show ethernet oam statistics](#), on page 223
- [show ethernet oam summary](#), on page 225
- [show interface](#), on page 227
- [show interface brief](#), on page 229
- [show interface capabilities](#), on page 231
- [show interface counters](#), on page 233
- [show interface counters brief](#), on page 236
- [show interface counters errors](#), on page 239
- [show interface counters storm-control](#), on page 243
- [show interface counters trunk](#), on page 245
- [show interface debounce](#), on page 246
- [show interface description](#), on page 248
- [show interface ethernet](#), on page 250
- [show interface flowcontrol](#), on page 253
- [show interface mgmt](#), on page 255
- [show interface port-channel](#), on page 257
- [show interface port-channel counters](#), on page 260
- [show interface status](#), on page 264
- [show interface switchport](#), on page 267
- [show interface transceiver](#), on page 269
- [show interface trunk](#), on page 271
- [show interface tunnel](#), on page 273
- [show ip dhcp snooping statistics](#), on page 274
- [show lacp counters](#), on page 275
- [show lacp interface](#), on page 276
- [show lacp neighbor](#), on page 278
- [show lacp port-channel](#), on page 279

- [show lacp summary](#), on page 280
- [show lacp system-identifier](#), on page 282
- [show ospfv3](#), on page 283
- [show port-channel compatibility-parameters](#), on page 285
- [show port-channel database](#), on page 287
- [show port-channel load-balance](#), on page 289
- [show port-channel rbh-distribution](#), on page 290
- [show port-channel summary](#), on page 291
- [show port-channel traffic](#), on page 293
- [show port-channel usage](#), on page 294
- [show port-profile](#), on page 295
- [show running-config bfd](#), on page 297
- [show running-config interface](#), on page 298
- [show running-config interface mgmt](#), on page 300
- [show running-config vpc](#), on page 301
- [show running-config vpc-config-sync](#), on page 302
- [show startup-config interface](#), on page 303
- [show startup-config vpc](#), on page 305
- [show udd](#), on page 306
- [show vdc](#), on page 307
- [show vpc brief](#), on page 308
- [show vpc config-sync](#), on page 312
- [show vpc consistency-parameters](#), on page 315
- [show vpc orphan-ports](#), on page 318
- [show vpc peer-keepalive](#), on page 320
- [show vpc role](#), on page 322
- [show vpc statistics](#), on page 324

show bfd neighbors

To display information about Bidirectional Forwarding Detection (BFD) neighbors, use the **show bfd neighbors** command.

```
show bfd neighbors [{multihop | application name | {dest-ip | src-ip} ipaddr interface int-if] |
[vrf vrf-name]} [details]
```

Syntax Description	Parameter	Description
	multihop	(Optional) Displays BFD multihop session details.
	application <i>name</i>	(Optional) Displays BFD information for the named protocol that BFD is enabled on.
	dest-ip <i>ipaddr</i>	(Optional) Displays BFD information for the destination IP address. The IP address is in dotted decimal notation for IPv4 and in A:B::C:D format for IPv6.
	src-ip <i>ipaddr</i>	(Optional) Displays BFD information for the source IP address. The IP address is in dotted decimal notation for IPv4 and in A:B::C:D format for IPv6.
	interface <i>int-if</i>	(Optional) Displays BFD information for the interface. Use the ? keyword to display a list of supported interfaces.
	vrf <i>vrf-name</i>	(Optional) Displays BFD information for the virtual routing and forwarding (VRF) instance.
	details	(Optional) Displays detailed BFD information.

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	8.1(1)	The multihop keyword was added.
	5.0(2)	This command was introduced.

Usage Guidelines Use the **show bfd neighbors** command to display information about BFD sessions. If you use the applications keyword, the application name is one of the following:

- bfd_app (bfd_app is a stub client and not real client)
- bgp
- eigrp
- hsrp
- isis
- ospf

- pim
- static

This command does not require a license.

Examples

This example shows how to display the output from the show bfd neighbors command:

```
switch# show bfd neighbors
OurAddr NeighAddr LD/RD RH/RS Holdown(mult) State Int
10.0.0.2 10.0.0.1 1124073474/1107296257 Up 582(3) Up Po10
```

This example shows how to display the output from the **show bfd neighbors application details** command for BFD:

```
switch# show bfd neighbors application bfd_app details
OurAddr NeighAddr LD/RD RH/RS Holdown(mult) State Int
1.1.1.2 1.1.1.1 1090519041/1107296257 Up 137(3) Up Eth4/37
Session state is Up and not using echo function
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000 us, MinRxInt: 50000 us, Multiplier: 3
Received MinRxInt: 50000 us, Received Multiplier: 3
Holdown (hits): 150 ms (2), Hello (hits): 50 ms (1232223)
Rx Count: 1267540, Rx Interval (ms) min/max/avg: 0/1789/44 last: 12 ms ago
Tx Count: 1232223, Tx Interval (ms) min/max/avg: 41/41/41 last: 13 ms ago
Registered protocols: bfd_app
Uptime: 0day 15hour 5minute 8second 430ms
Last packet: Version: 1 - Diagnostic: 0
              State bit: Up - Demand bit: 0
              Poll bit: 0 - Final bit: 0
              Multiplier: 3 - Length: 24
              My Discr.: 1107296257 - Your Discr.: 1090519041
              Min tx interval: 50000 - Min rx interval: 50000
              Min Echo interval: 0
```

This example shows how to display information about BFD multihop sessions:

```
switch# show bfd neighbors multihop details

OurAddr      NeighAddr      LD/RD          RH/RS          Holdown(mult)
State        Int            Vrf            Type           Up
200.1.1.1    100.1.1.1     1090519058/1107296266 Up             695(3)      Up
              default              MH

Session state is Up and not using echo function

Session type: Multihop
Local Diag: 0, Demand mode: 0, Poll bit: 0, Authentication: None
MinTxInt: 250000 us, MinRxInt: 250000 us, Multiplier: 20
Received MinRxInt: 250000 us, Received Multiplier: 3
Holdown (hits): 750 ms (2), Hello (hits): 250 ms (622317)
Rx Count: 714572, Rx Interval (ms) min/max/avg: 0/2210/196 last: 54 ms ago
Tx Count: 622317, Tx Interval (ms) min/max/avg: 187/187/187 last: 146 ms ago
Registered protocols: bgp
Uptime: 0 days 12 hrs 21 mins 59 secs
Last packet: Version: 1 - Diagnostic: 0
              State bit: Up - Demand bit: 0
              Poll bit: 0 - Final bit: 0
              Multiplier: 3 - Length: 24
              My Discr.: 1107296266 - Your Discr.: 1090519058
              Min tx interval: 250000 - Min rx interval: 250000
```

```

Min Echo interval: 0      - Authentication bit: 0
Hosting LC: 9, Down reason: None, Reason not-hosted: None, Offloaded: No

```

Table 4: `show bfd neighbors` Field Descriptions, on page 211 describes the significant fields shown in the display.

Table 4: `show bfd neighbors` Field Descriptions

Field	Description
OurAddr	IP address of the interface for which the <code>show bfd neighbors</code> command was entered.
NeighAddr	IPv4 or IPv6 address of the BFD adjacency or neighbor.
LD/RD	Local discriminator and remote discriminator being used for the session.
RH	Remote Heard—Indicates that the remote BFD neighbor has been heard.
Holdown(mult)	Detect timer multiplier that is used for this session.
State	State of the interface—Up or Down.
Int	Interface type and slot/port.
Session state is UP and not using echo function	BFD is up and not running in echo mode.
RX Count	Number of BFD control packets that have been received from the BFD neighbor.
TX Count	Number of BFD control packets that have been sent by the BFD neighbor.
TX Interval	Interval, in milliseconds, between sent BFD packets.
Registered protocols	Routing protocols that have been registered with BFD.
Last packet: Version:	BFD version detected and run between the BFD neighbors.
Diagnostic	<p>Diagnostic code specifying the local system's reason for the last transition of the session from Up to some other state.</p> <p>State values are as follows:</p> <ul style="list-style-type: none"> • 0—No Diagnostic • 1—Control Detection Time Expired • 2—Echo Function Failed • 3—Neighbor Signaled Session Down • 4—Forwarding Plane Reset • 5—Path Down • 6—Concentrated Path Down • 7—Administratively Down

Field	Description
Demand bit	Demand Mode bit. If set, the transmitting system wants to operate in demand mode. BFD has two modes—asynchronous and demand. The Cisco implementation of BFD supports only asynchronous mode.
Poll bit	Poll bit. If the Poll bit is set, the transmitting system is requesting verification of connectivity or of a parameter change.
Final bit	Final bit. If the Final bit is set, the transmitting system is responding to a received BFD control packet that had a Poll (P) bit set.
Multiplier	<p>Detect time multiplier. The negotiated transmit interval, multiplied by the detect time multiplier, determines the detection time for the transmitting system in BFD asynchronous mode.</p> <p>The detect time multiplier is similar to the hello multiplier in Intermediate System-to-Intermediate System (IS-IS), which is used to determine the hold timer: (hello interval) * (hello multiplier) = hold timer. If a hello packet is not received within the hold-timer interval, a failure has occurred.</p> <p>Similarly, for BFD: (transmit interval) * (detect multiplier) = detect timer. If a BFD control packet is not received from the remote system within the detect-timer interval, a failure has occurred.</p>
Length	Length of the BFD control packet, in bytes.
My Discr.	My Discriminator. Unique, nonzero discriminator value generated by the transmitting system used to demultiplex multiple BFD sessions between the same pair of systems.
Your Discr.	Your Discriminator. The discriminator received from the corresponding remote system. This field reflects the received value of My Discriminator or is zero if that value is unknown.
Min tx interval	Minimum transmission interval, in microseconds, that the local system wants to use when sending BFD control packets.
Min rx interval	Minimum receipt interval, in microseconds, between received BFD control packets that the system can support.
Min Echo interval	Minimum interval, in microseconds, between received BFD control packets that the system can support. If the value is zero, the transmitting system does not support the receipt of BFD echo packets.
Vrf	Virtual routing and forwarding instance (VRF). The BFD session belongs to the specified VRF.
Type	Session type. The session type is either single hop (SH) or multihop (MH).

Related Commands

Command	Description
bfd echo	Enables BFD echo mode.

show cfs application

To display information about applications that are currently enabled to use Cisco Fabric Services (CFS) distribution, use the **show cfs application** command.

show cfs application [**name** *application_name*]

Syntax Description	name <i>application_name</i>	(Optional) Displays the name of a specific application.
---------------------------	--	---

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	7.1(1)D1(0)	The output of the command was updated.
	4.1(2)	This command was introduced.

Usage Guidelines This command does not require a license.

Examples

This example shows how to display CFS information about applications that are currently enabled to use CFS distribution:

```
switch# show cfs application
-----
Application      Enabled      Scope
-----
ntp              No          Physical-fc-ip
stp              Yes         Physical-eth
vpc              Yes         Physical-eth
vpc-config-sync Yes         Physical-eth
igmp             Yes         Physical-eth
l2fm             Yes         Physical-eth
role             No          Physical-fc-ip
radius          No          Physical-fc-ip
callhome        Yes         Physical-fc-ip
Total number of entries = 9
```

This example shows how to display CFS information about the Call Home application:

```
switch# show cfs application name callhome
Enabled          : Yes
Timeout          : 20s
Merge Capable    : Yes
Scope            : Physical-fc-ip
Region           : 4
```

Related Commands	Command	Description
	show <i>application_name</i> session status	Displays the CFS configuration session status for the application, including the last action, the result, and the reason if there was a failure.
	show cfs internal	Displays information internal to CFS including memory statistics, event history, and so on.
	show cfs lock	Displays all active CFS fabric locks.
	show cfs merge status name	Displays the merge status for a given CFS application.
	show cfs peers	Displays all the CFS peers in the physical fabric.
	show cfs regions	Displays all the CFS applications with peers and region information.
	show cfs status	Displays the status of CFS distribution on the device as well as IP distribution information.
	show tech-support cfs	Displays information about the CFS configuration required by technical support when resolving a CFS issue.
	show logging level cfs	Displays the CFS logging configuration.

show errdisable

To display the errdisable recovery and detection run-time information, use the **show errdisable** command.

show errdisable {detect | recovery}

Syntax Description	detect	recovery
	Enables errdisable detection on all causes.	Enables automatic errdisable recovery from all causes.

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	6.2(2)	This command was introduced.

Usage Guidelines This command does not require a license.

Examples This example shows how to display errdisable detection on all cases:

```
switch# show errdisable detect
ErrDisable Reason          Timer Status
-----
link-flap                  enabled
udld                      enabled
bpduguard                 enabled
loopback                  enabled
storm-ctrl                enabled
sec-violation             enabled
psec-violation            enabled
vpc-peerlink              enabled
failed-port-state        enabled
event-debug               enabled
event-debug1              enabled
event-debug2              enabled
event-debug3              enabled
event-debug4              enabled
switch#
```

This example shows how to display errdisable recovery for all the cases:

```
switch# show errdisable recovery
ErrDisable Reason          Timer Status
-----
link-flap                  disabled
udld                      disabled
bpduguard                 disabled
loopback                  disabled
storm-ctrl                disabled
sec-violation             disabled
psec-violation            disabled
vpc-peerlink              disabled
failed-port-state        disabled
```

show errdisable

```
event-debug disabled
event-debug1 disabled
event-debug2 disabled
event-debug3 disabled
event-debug4 disabled
Timer interval: 300
switch#
```

Related Commands

Command	Description
bfd echo	Enables BFD echo mode.

show ethernet oam configuration

To display the current active Ethernet OAM configuration on an interface, use the **show ethernet oam configuration** command in EXEC mode.

show ethernet oam configuration [**interface** *type interface-path-id*]

Syntax Description	interface <i>type</i>	(Optional) Displays information about the specified interface type.
	<i>interface-path-id</i>	(Optional) Physical interface or virtual interface.
	Note	Use the show interfaces command to see a list of all interfaces currently configured on the switch.

Command Default If no parameters are specified, the configurations for all Ethernet OAM interfaces is displayed.

Command Modes EXEC mode.

Supported User Roles

network-admin

vdc--admin

network---operator

vdc-operator

Command History	Release	Modification
	7.3(0)D1(1)	This command was introduced.

Usage Guidelines This command displays the Ethernet OAM configuration information for all interfaces, or a specified interface. This command does not require a license.

The following example shows how to display Ethernet OAM configuration information for a specific interface:

```
switch# show ethernet oam configuration interface ethernet 2/19
```

```
Thu Aug 5 21:54:34.050 DST
Ethernet2/19:
Hello interval: 1s
Link monitoring enabled: Y
Remote loopback enabled: N
Mib retrieval enabled: N
Uni-directional link-fault detection enabled: N
Configured mode: Active
Connection timeout: 5
Symbol period window: 0
Symbol period low threshold: 1
Symbol period high threshold: None
Frame window: 1000
Frame low threshold: 1
```

```

Frame high threshold: None
Frame period window: 1000
Frame period low threshold: 1
Frame period high threshold: None
Frame seconds window: 60000
Frame seconds low threshold: 1
Frame seconds high threshold: None
High threshold action: None
Link fault action: Log
Dying gasp action: Log
Critical event action: Log
Discovery timeout action: Log
Capabilities conflict action: Log
Wiring conflict action: Error-Disable
Session up action: Log
Session down action: Log
Remote loopback action: Log
Require remote mode: Ignore
Require remote MIB retrieval: N
Require remote loopback support: N
Require remote link monitoring: N

```

The following example shows how to display the configuration for all EOAM interfaces:

```

switch# show ethernet oam configuration

Thu Aug 5 22:07:06.870 DST
Ethernet2/19:
Hello interval: 1s
Link monitoring enabled: Y
Remote loopback enabled: N
Mib retrieval enabled: N
Uni-directional link-fault detection enabled: N
Configured mode: Active
Connection timeout: 5
Symbol period window: 0
Symbol period low threshold: 1
Symbol period high threshold: None
Frame window: 1000
Frame low threshold: 1
Frame high threshold: None
Frame period window: 1000
Frame period low threshold: 1
Frame period high threshold: None
Frame seconds window: 60000
Frame seconds low threshold: 1
Frame seconds high threshold: None
High threshold action: None
Link fault action: Log
Dying gasp action: Log
Critical event action: Log
Discovery timeout action: Log
Capabilities conflict action: Log
Wiring conflict action: Error-Disable
Session up action: Log
Session down action: Log
Remote loopback action: Log
Require remote mode: Ignore
Require remote MIB retrieval: N
Require remote loopback support: N
Require remote link monitoring: N

```

show ethernet oam discovery

To display the currently configured OAM information of Ethernet OAM sessions on interfaces, use the **show ethernet oam discovery** command in EXEC mode.

```
show ethernet oam discovery [{brief| [brief] interface type interface-path-id}]
```

Syntax Description	brief	Displays minimal, currently configured OAM information in table form.
	interfacetype	(Optional) Displays information about the specified interface type.
	<i>interface-path-id</i>	Physical interface or virtual interface.
	Note	Use the show interfaces command to see a list of all interfaces currently configured on the switch.

Command Default Displays detailed information for Ethernet OAM sessions on all interfaces.

Command Modes EXEC mode

Supported User Roles

network-admin
vdc--admin
network--operator
vdc-operator

Command History	Release	Modification
	7.3(0)D1(1)	This command was introduced.

Usage Guidelines This command does not require a license.

The following example shows how to display the minimal, currently configured OAM information for Ethernet OAM sessions on all interfaces:

```
switch# show ethernet oam discovery brief
```

```
Sat Jul 4 13:52:42.949 PST
Flags:
L - Link Monitoring support
M - MIB Retrieval support
R - Remote Loopback support
U - Unidirectional detection support
* - data is unavailable
```

```
Local
Interface Remote MAC Address Remote Vendor Mode Capability
-----
```

```

Gi0/1/5/1  0010.94fd.2bfa  00000A Active      L
Gi0/1/5/2  0020.95fd.3bfa  00000B Active      M
Gi0/1/6/1  0030.96fd.6bfa  00000C Passive     L R
Fa0/1/3/1  0080.09ff.e4a0  00000C Active      L R

```

The following example shows how to display detailed, currently configured OAM information for the Ethernet OAM session on a specific interface:

```
switch# show ethernet oam discovery interface ethernet 2/19
```

```

Sat Jul 4 13:56:49.967 PST
Ethernet2/19:
Local client
-----
Administrative configuration:
PDU revision: 1
Mode: Active
Unidirectional support: N
Link monitor support: Y
Remote loopback support: N
MIB retrieval support: N
Maximum PDU size: 1500
Mis-wiring detection key: 5E9D
Operational status:
Port status: Active send
Loopback status: None
Interface mis-wired: N

Remote client
-----
MAC address: 0030.96fd.6bfa
Vendor (OUI): 00.00.0C (Cisco)
Administrative configuration:
PDU revision: 5
Mode: Passive
Unidirectional support: N
Link monitor support: Y
Remote loopback support: Y
MIB retrieval support: N
Maximum PDU size: 1500

```

Related Commands

Command	Description
show ethernet oam configuration	Displays the current active Ethernet OAM configuration on an interface
show ethernet oam statistics	Displays the local and remote Ethernet OAM statistics for interfaces.
show ethernet oam interfaces	Displays the current state of Ethernet OAM interfaces.

show ethernet oam event-log

To display the most recent OAM event logs per interface, use the **show ethernet oam event-log** command in EXEC mode.

```
show ethernet oam event-log [{detail | [detail] interface type interface-path-id}]
```

Syntax Description	
interface <i>typeinterface-path-id</i>	Filters the output to only include events for the specified interface.
detail	Displays additional details like threshold value, breaching value, total running errors and window size of a particular interface.

Command Default This command displays event logs for all interfaces which have OAM configured.

Command Modes EXEC mode.

Supported User Roles

network-admin
vdc--admin
network--operator
vdc-operator

Command History	Release	Modification
	7.3(0)D1(1)	This command was introduced.

Usage Guidelines This command does not require a license.

The following example shows how to display the event logs for all interfaces which have OAM configured:

```
switch# show ethernet oam event-log

Wed Jan 23 06:16:46.684 PST
Local Action Taken:
N/A - No action needed EFD - Interface brought down using EFD
None - No action taken Err.D - Interface error-disabled
Logged - System logged

Ethernet2/19
=====
Time                Type                Loc'n  Action  Threshold  Breaching Value
-----
Wed Jan 23 06:13:25 PST Symbol period      Local   N/A     1          4
Wed Jan 23 06:13:33 PST Frame             Local   N/A     1          6
Wed Jan 23 06:13:37 PST Frame period     Local   None    9         12
Wed Jan 23 06:13:45 PST Frame seconds   Local   N/A     1         10
Wed Jan 23 06:13:57 PST Dying gasp       Remote  Logged  N/A       N/A
```

show ethernet oam event-log

Ethernet2/20

```

=====
Time                               Type           Loc'n  Action  Threshold Breaching Value
-----
Wed Jan 23 06:26:14 PST           Dying gasp     Remote Logged  N/A      N/A
Wed Jan 23 06:33:25 PST           Symbol period  Local   N/A      1         4
Wed Jan 23 06:43:33 PST           Frame period   Remote  N/A      9         12
Wed Jan 23 06:53:37 PST           Critical event Remote  Logged  N/A      N/A
Wed Jan 23 07:13:45 PST           Link fault     Remote  EFD     N/A      N/A
Wed Jan 23 07:18:23 PST           Dying gasp     Local   Logged  N/A      N/A

```

Related Commands

Command	Description
show ethernet oam configuration	Displays the current active Ethernet OAM configuration on an interface.
show ethernet oam discovery	Displays the current status of Ethernet OAM sessions.
show ethernet oam interfaces	Displays the current state of Ethernet OAM interfaces.

show ethernet oam statistics

To display the local and remote Ethernet OAM statistics for interfaces, use the **show ethernet oam statistics** command in EXEC mode.

show ethernet oam statistics [**interface type interface-path-id**]

Syntax Description	interface type (Optional) Displays information about the specified interface type. For more information, use the question mark (?) online help function.
	interface-path-id Physical interface or virtual interface.
	Note Use the show interfaces command to see a list of all interfaces currently configured on the switch.

Command Default No parameters displays statistics for all Ethernet OAM interfaces.

Command Modes EXEC mode.

Supported User Roles

network-admin
vdc--admin
network--operator
vdc-operator

Command History	Release	Modification
	7.3(0)D1(1)	This command was introduced.

Usage Guidelines This command does not require a license.

The following example shows how to display Ethernet OAM statistics for a specific interface:

```
switch# show ethernet oam statistics interface ethernet 2/19

Ethernet2/19:
Counters
-----
Information OAMPDU Tx 161177
Information OAMPDU Rx 151178
Unique Event Notification OAMPDU Tx 0
Unique Event Notification OAMPDU Rx 0
Duplicate Event Notification OAMPDU Tx 0
Duplicate Event Notification OAMPDU Rx 0
Loopback Control OAMPDU Tx 0
Loopback Control OAMPDU Rx 0
Variable Request OAMPDU Tx 0
Variable Request OAMPDU Rx 0
Variable Response OAMPDU Tx 0
Variable Response OAMPDU Rx 0
```

show ethernet oam statistics

```

Organization Specific OAMPDU Tx 0
Organization Specific OAMPDU Rx 0
Unsupported OAMPDU Tx 45
Unsupported OAMPDU Rx 0
Frames Lost due to OAM 23
Fixed frames Rx 1

```

Local event logs

```
-----
```

```

Errored Symbol Period records 0
Errored Frame records 0
Errored Frame Period records 0
Errored Frame Second records 0

```

Remote event logs

```
-----
```

```

Errored Symbol Period records 0
Errored Frame records 0
Errored Frame Period records 0
Errored Frame Second records 0

```

Related Commands

Command	Description
show ethernet oam configuration	Displays the current active Ethernet OAM configuration on an interface.
show ethernet oam discovery	Displays the current status of Ethernet OAM sessions.
show ethernet oam interfaces	Displays the current state of Ethernet OAM interfaces.

show ethernet oam summary

To display a summary of all the active OAM sessions on a switch, use the **show ethernet oam summary** command in privileged EXEC mode.

show ethernet oam summary [detail]

Syntax Description	detail Displays the 10 most recent events across all interfaces along with the action taken.				
Command Default	None				
Command Modes	Privileged EXEC (#)				
	Supported User Roles				
	network-admin				
	vdc--admin				
	network--operator				
	vdc-operator				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>7.3(0)D1(1)</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	7.3(0)D1(1)	This command was introduced.
Release	Modification				
7.3(0)D1(1)	This command was introduced.				
Usage Guidelines	This command does not require a license.				

The following example shows how to display a summary of all the active OAM sessions on a switch:

```
switch# show ethernet oam summary
```

```
Link OAM System Summary
=====
Profiles 6
Interfaces 10
Interface states:
Port down 1
Passive wait 1
Active send 1
[Evaluating 0]
[Local accept 0]
[Local reject 0]
Remote reject 1
Operational 6
Loopback mode 1
Miswired connections 1
Events 13
Local 4
Symbol error 0
Frame 2
Frame period 1
Frame seconds 1
Remote 9
Symbol error 3
```

```
Frame 4
Frame period 1
Frame seconds 1
```

The following example shows how to use the detail keyword to display the 10 most recent events across all interfaces along with the action taken:

```
switch# show ethernet oam summary detail
```

```
Link OAM System Summary
=====
```

```
Profiles 6
Interfaces 10
Interface states:
Port down 1
Passive wait 1
Active send 1
[Evaluating 0]
[Local accept 0]
[Local reject 0]
Remote reject 1
Operational 6
Loopback mode 1
Miswired connections 1
Events 13
Local 4
Symbol error 0
Frame 2
Frame period 1
Frame seconds 1
Remote 9
Symbol error 3
Frame 4
Frame period 1
Frame seconds 1
```

```
Recent Event Logs
=====
```

Interface	Time	Type	Loc'n	Action
Gi0/0/0/0	Jan 23 06:13:25	PST Symbol period	Local	N/A
Gi0/0/0/0	Jan 23 06:13:33	PST Frame	Local	N/A
Gi0/0/0/2	Jan 23 06:13:37	PST Frame period	Local	N/A
Gi0/0/0/1	Jan 23 06:13:45	PST Frame seconds	Local	EFD
Gi0/0/0/0	Jan 23 06:13:48	PST Dying gasp	Remote	Err.D

Related Commands

Command	Description
ethernetoamprofile	Creates an EOAM profile and enters EOAM configuration mode.
featureethernet-link-oam	Enables the ethernet link OAM feature.
require-remote	Enters the ethernet OAM require-remote configuration submode to specify the features that you have to enable before an OAM session can become active.

show interface

To display the interface status and information, use the **show interface** command..

show interface

Syntax Description

This command has some keywords. For more details, see the “Usage Guidelines” section for this command.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.1(1)	Changed the show interface command output.
5.1(1)	Changed the command output to show the port is suspended due to min-links.
4.0	This command was introduced.

Usage Guidelines

Use the show interface command to display the interface status and information. To display **show interface** commands with valid keywords, see the following commands in this document:

- **show interface brief**—Displays brief information of interface.
- **show interface capabilities**—Displays interface capabilities information.
- **show interface counters**—Displays interface counters.
- **show interface counters brief**—Displays input and output rates for interface counters.
- **show interface counters detailed**—Displays only nonzero counters.
- **show interface counters errors**—Displays interface error counters.
- **show interface counters module**—Displays interface counters on a specified module.
- **show interface counters snmp**—Displays SNMP MIB values.
- **show interface counters storm-control**—Displays interface storm-control counters.
- **show interface counters trunk**—Displays interface trunk counters.
- **show interface debounce**—Displays interface debounce time information.
- **show interface description**—Displays interface description.
- **show interface ethernet**—Displays Ethernet interface information.
- **show interface flowcontrol**—Displays interface flow control information.
- **show interface mgmt**—Displays management interface.
- **show interface port-channel**—Displays port-channel interface.
- **show interface port-channel counters**—Displays interface port-channel counters.

- **show interface status**—Displays the interface line status.
- **show interface switchport**—Displays interface switchport information.
- **show interface transceiver**—Displays interface transceiver information.
- **show interface trunk**—Displays interface trunk information.

This command does not require a license.

Examples

This example shows how to display the enhanced show output for the sub-interfaces. The output is enhanced beginning with Cisco NX-OS Release 6.1(1):

```
switch# show interface ethernet 101/1/1
Ethernet101/1/1 is up
admin state is up,
  Hardware: 100/1000 Ethernet, address: 1cdf.0f3b.8042 (bia 1cdf.0f3b.8042)
  MTU 9216 bytes, BW 1000000 Kbit, DLY 10 usec
  reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, medium is broadcast
  Port mode is trunk
  full-duplex, 1000 Mb/s
  Beacon is turned off
  Auto-Negotiation is turned on
  Input flow-control is off, output flow-control is on
  Auto-mdix is turned off
  Switchport monitor is off
  EtherType is 0x8100
  Last link flapped 2d16h
  Last clearing of "show interface" counters never
  2 interface resets
  30 seconds input rate 64 bits/sec, 0 packets/sec
  30 seconds output rate 72 bits/sec, 0 packets/sec
  Load-Interval #2: 5 minute (300 seconds)
    input rate 64 bps, 0 pps; output rate 72 bps, 0 pps
RX
  0 unicast packets  6331 multicast packets  0 broadcast packets
  6331 input packets  519142 bytes
  0 jumbo packets  0 storm suppression packets
  0 runts  0 giants  0 CRC  0 no buffer
  0 input error  0 short frame  0 overrun  0 underrun  0 ignored
  0 watchdog  0 bad etype drop  0 bad proto drop  0 if down drop
  0 input with dribble  0 input discard
  0 Rx pause
TX
  0 unicast packets  2124 multicast packets  16 broadcast packets
  2140 output packets  576661 bytes
  0 jumbo packets
  0 output error  0 collision  0 deferred  0 late collision
  0 lost carrier  0 no carrier  0 babble  0 output discard
  0 Tx pause
switch#
```

Related Commands

Command	Description
interface	Enters the interface configuration mode and configures the types and identities of interfaces .

show interface brief

To display brief information about the interface, use the **show interface brief** command.

show interface [{**ethernet** *slot-port* | **port-channel** *channel-number*}]

Syntax Description	Parameter	Description
	ethernet	(Optional) Specifies the slot and port of the Ethernet interface that you want to display.
	<i>slot/port</i>	(Optional) Slot number and port number for the Ethernet interface. The range is from 1 to 253.
	port-channel	(Optional) Specifies the port-channel number of the port-channel interface that you want to display.
	<i>channel-number</i>	(Optional) Channel number. The range is from 1 to 4096.

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	4.0	This command was introduced.

Usage Guidelines If you do not specify an interface, this command displays information about all Layer 2 interfaces. Use the **show interface brief** command to display brief information about the interface.

This command does not require a license.

Examples

This example shows how to display brief information about the interface:

```
switch# show interface brief
-----
Port    VRF      Status IP Address                               Speed  MTU
-----
mgmt0   --      up     172.28.231.193                           1000   1500
-----
Ethernet VLAN  Type Mode  Status Reason                                Speed  Port
Interface                                     Ch #
-----
Eth2/1   --    eth  routed down  Administratively down  auto(D) --
Eth2/2   --    eth  routed down  Administratively down  auto(D) --
Eth2/3   --    eth  routed down  Administratively down  auto(D) --
Eth2/4   1     eth  pvlan down  Administratively down  auto(D) --
Eth2/5   --    eth  routed down  Administratively down  auto(D) --
Eth2/6   1     eth  access down  Link not connected     auto(D) --
Eth2/7   1     eth  access up    none                   1000(D) --
Eth2/8   --    eth  routed down  Administratively down  auto(D) --
Eth2/9   1     eth  access up    none                   1000(D) --
Eth2/10  1     eth  access down  Link not connected     auto(D) --
Eth2/11  --    eth  routed down  Administratively down  auto(D) --
Eth2/12  --    eth  routed down  Administratively down  auto(D) --
Eth2/13  --    eth  routed down  Administratively down  auto(D) --
```

show interface brief

```

Eth2/14      --      eth  routed down  Administratively down  auto(D) --
Eth2/15      --      eth  routed down  Administratively down  auto(D) --
Eth2/16      --      eth  routed down  Administratively down  auto(D) --
Eth2/17      --      eth  routed down  Administratively down  auto(D) --
Eth2/18      --      eth  routed down  Administratively down  auto(D) --
Eth2/19      --      eth  routed down  Administratively down  auto(D) --
Eth2/20      --      eth  routed down  Administratively down  auto(D) --
Eth2/21      --      eth  routed down  Administratively down  auto(D) --
Eth2/22      --      eth  routed down  Administratively down  auto(D) --
Eth2/23      --      eth  routed down  Administratively down  auto(D) --
Eth2/24      --      eth  routed down  Administratively down  auto(D) --
Eth2/25      --      eth  routed down  Administratively down  auto(D) --
Eth2/26      --      eth  routed down  Administratively down  auto(D) --
Eth2/27      --      eth  routed down  Administratively down  auto(D) --
Eth2/28      --      eth  routed down  Administratively down  auto(D) --
Eth2/29      --      eth  routed down  Administratively down  auto(D) --
Eth2/30      --      eth  routed down  Administratively down  auto(D) --
Eth2/31      --      eth  routed down  Administratively down  auto(D) --
Eth2/32      --      eth  routed down  Administratively down  auto(D) --
Eth2/33      --      eth  routed down  Administratively down  auto(D) --
Eth2/34      --      eth  routed down  Administratively down  auto(D) --
Eth2/35      --      eth  routed down  Administratively down  auto(D) --
Eth2/36      --      eth  routed down  Administratively down  auto(D) --
Eth2/37      --      eth  routed down  Administratively down  auto(D) --
Eth2/38      --      eth  routed down  Administratively down  auto(D) --
Eth2/39      --      eth  routed down  Administratively down  auto(D) --
Eth2/40      --      eth  routed down  Administratively down  auto(D) --
Eth2/41      --      eth  routed down  Administratively down  auto(D) --
Eth2/42      --      eth  routed down  Administratively down  auto(D) --
Eth2/43      --      eth  routed down  Administratively down  auto(D) --
Eth2/44      --      eth  routed down  Administratively down  auto(D) --
Eth2/45      --      eth  routed down  Administratively down  auto(D) --
Eth2/46      --      eth  routed down  Administratively down  auto(D) --
Eth2/47      --      eth  routed down  Administratively down  auto(D) --
Eth2/48      --      eth  routed down  Administratively down  auto(D) --

```

```

-----
Interface      Secondary VLAN (Type)      Status      Reason
-----
Vlan1          --                          down        none

```

Related Commands

Command	Description
interface	Enters the interface configuration mode and configures the types and identities of interfaces.

show interface capabilities

To display information about the interface capabilities, use the **show interface capabilities** command.

show interface [{**ethernet** *slot-port* | **port-channel** *channel-number*}]**capabilities**

Syntax Description	Parameter	Description
	ethernet	(Optional) Specifies the slot and port of the Ethernet interface that you want to display.
	<i>slot/port</i>	(Optional) Slot number and port number for the Ethernet interface. The range is from 1 to 253.
	port-channel	(Optional) Specifies the port-channel number of the port-channel interface that you want to display.
	<i>channel-number</i>	(Optional) Channel number. The range is from 1 to 4096.

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	4.0	This command was introduced.

Usage Guidelines Use the **show interface capabilities** command to display information about the capabilities of the interface such as the speed, duplex, and rate mode. If you do not specify an interface, this command displays information about all Layer 2 interfaces.

This command does not require a license.

Examples

This example shows how to display the capabilities for a specific interface:

```
switch# show interface ethernet 2/7 capabilities
Ethernet2/7
  Model:                COPPER
  Type:                 1000BaseT
  Speed:                10,100,1000,auto
  Duplex:               half/full/auto
  Trunk encap. type:    802.1Q
  Channel:              yes
  Broadcast suppression: percentage(0-100)
  Flowcontrol:          rx-(off/on/desired),tx-(off/on/desired)
  Rate mode:            dedicated
  QOS scheduling:       rx-(2q4t),tx-(1p3q4t)
  CoS rewrite:          yes
  ToS rewrite:          yes
  SPAN:                 yes
  UDLD:                 yes
  Link Debounce:        yes
  Link Debounce Time:   yes
  MDIX:                 yes
  Port Group Members:   none
```

Related Commands

Command	Description
interface	Enters the interface configuration mode and configures the types and identities of interfaces.

show interface counters

To display in and out counters for all interfaces in the system, use the **show interface counters** command.

show interface [{**ethernet** *slot-port* | **port-channel** *channel-number*}]**counters**

Syntax Description	Parameter	Description
	ethernet	(Optional) Specifies the slot and port of the Ethernet interface that you want to display.
	<i>slot/port</i>	(Optional) Slot number and port number for the Ethernet interface. The range is from 1 to 253.
	port-channel	(Optional) Specifies the port-channel number of the port-channel interface that you want to display.
	<i>channel-number</i>	(Optional) Channel number. The range is from 1 to 4096.

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	4.0	This command was introduced.

Usage Guidelines Use the **show interface counters** command to display in and out counters for all or a specific interface. If you do not specify an interface, this command displays information about all Layer 2 interfaces.

This command does not require a license.

Examples

This example shows how to display the in and out counters for all interfaces:

```
switch# show interface counters
-----
Port                InOctets      InUcastPkts   InMcastPkts   InBcastPkts
-----
mgmt0                137046816     46882         115497         267729
Eth2/1                0             0             0             0
Eth2/2                0             0             0             0
Eth2/3                0             0             0             0
Eth2/4                0             0             0             0
Eth2/5                0             0             0             0
Eth2/6                0             0             0             0
Eth2/7                295061        0             1348          0
Eth2/8                0             0             0             0
Eth2/9                4174381      0             53303         0
Eth2/10              0             0             0             0
Eth2/11              0             0             0             0
Eth2/12              0             0             0             0
Eth2/13              0             0             0             0
Eth2/14              0             0             0             0
Eth2/15              0             0             0             0
Eth2/16              0             0             0             0
Eth2/17              0             0             0             0
```

show interface counters

Eth2/18	0	0	0	0
Eth2/19	0	0	0	0
Eth2/20	0	0	0	0
Eth2/21	0	0	0	0
Eth2/22	0	0	0	0
Eth2/23	0	0	0	0
Eth2/24	0	0	0	0
Eth2/25	0	0	0	0
Eth2/26	0	0	0	0
Eth2/27	0	0	0	0
Eth2/28	0	0	0	0
Eth2/29	0	0	0	0
Eth2/30	0	0	0	0
Eth2/31	0	0	0	0
Eth2/32	0	0	0	0
Eth2/33	0	0	0	0
Eth2/34	0	0	0	0
Eth2/35	0	0	0	0
Eth2/36	0	0	0	0
Eth2/37	0	0	0	0
Eth2/38	0	0	0	0
Eth2/39	0	0	0	0
Eth2/40	0	0	0	0
Eth2/41	0	0	0	0
Eth2/42	0	0	0	0
Eth2/43	0	0	0	0
Eth2/44	0	0	0	0
Eth2/45	0	0	0	0
Eth2/46	0	0	0	0
Eth2/47	0	0	0	0
Eth2/48	0	0	0	0
Vlan1	0	0	0	--

Port	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts
mgmt0	7555343	45951	1352	136
Eth2/1	0	0	0	0
Eth2/2	0	0	0	0
Eth2/3	0	0	0	0
Eth2/4	0	0	0	0
Eth2/5	0	0	0	0
Eth2/6	0	0	0	0
Eth2/7	4174381	0	53303	0
Eth2/8	0	0	0	0
Eth2/9	295061	0	1348	0
Eth2/10	0	0	0	0
Eth2/11	0	0	0	0
Eth2/12	0	0	0	0
Eth2/13	0	0	0	0
Eth2/14	0	0	0	0
Eth2/15	0	0	0	0
Eth2/16	0	0	0	0
Eth2/17	0	0	0	0
Eth2/18	0	0	0	0
Eth2/19	0	0	0	0
Eth2/20	0	0	0	0
Eth2/21	0	0	0	0
Eth2/22	0	0	0	0
Eth2/23	0	0	0	0
Eth2/24	0	0	0	0
Eth2/25	0	0	0	0
Eth2/26	0	0	0	0
Eth2/27	0	0	0	0
Eth2/28	0	0	0	0

```

Eth2/29          0          0          0          0
Eth2/30          0          0          0          0
Eth2/31          0          0          0          0
Eth2/32          0          0          0          0
Eth2/33          0          0          0          0
Eth2/34          0          0          0          0
Eth2/35          0          0          0          0
Eth2/36          0          0          0          0
Eth2/37          0          0          0          0
Eth2/38          0          0          0          0
Eth2/39          0          0          0          0
Eth2/40          0          0          0          0
Eth2/41          0          0          0          0
Eth2/42          0          0          0          0
Eth2/43          0          0          0          0
Eth2/44          0          0          0          0
Eth2/45          0          0          0          0
Eth2/46          0          0          0          0
Eth2/47          0          0          0          0
Eth2/48          0          0          0          0
Vlan1            0          0          0          0
  
```

Related Commands

Command	Description
clear counters interface	Clears the counters for the specified interfaces.

show interface counters brief

To display input and output rates for all interfaces in the system, use the **show interface counter brief** command.

show interface [{**ethernet** *slot-port* | **port-channel** *channel-number*}]**countersbrief**
load-interval[**counter** {**1** | **2** | **3**}]

Syntax Description

ethernet	(Optional) Specifies the slot and port of the Ethernet interface that you want to display.
<i>slot/port</i>	(Optional) Slot number and port number for the Ethernet interface. The range is from 1 to 253.
port-channel	(Optional) Specifies the port-channel number of the port-channel interface that you want to display.
<i>channel-number</i>	(Optional) Channel number. The range is from 1 to 4096.
load-interval	(Optional) Specifies the sampling interval for statistics collections on interfaces.
counter	(Optional) Specifies the counter for this load interval.
1 2 3	Specifies the counter number configured on the interface.

Command Default

1—30 seconds; 60 seconds for VLAN network interface
 2—300 seconds
 3—not configured

Command Modes

Any command mode

Command History

Release	Modification
6.2(8)	This command was introduced.

Usage Guidelines

Use the **show interface counters brief** command to display input and output rates for all or a specific interface. If you do not specify an interface, this command displays information about all interfaces. To change the counter from the default number of seconds, use the **load-interval** command.

This command does not require a license.

Examples

These examples show how to display the input and output rates for the interfaces:

```
switch# show interface counters brief
```

```
-----
Interface          Input Rate (avg)      Output Rate (avg)
-----
Rate      Total      Rate      Total      Rate averaging
MB/s      Frames      MB/s      Frames      interval (seconds)
-----
```

Eth6/1	0	0	0	0	30
	0	0	0	0	300
Eth6/2	0	0	0	0	30
	0	0	0	0	300
Eth6/3	0	0	0	0	30
	0	0	0	0	300
Eth6/4	0	0	0	0	30
	0	0	0	0	300
Eth6/5	0	0	0	0	30
	0	0	0	0	300
Eth6/6	0	0	0	0	30
	0	0	0	0	300
Eth6/7	0	0	0	0	30
	0	0	0	0	300
Eth6/8	0	0	0	0	30
	0	0	0	0	300
Eth6/9	0	0	0	0	30
	0	0	0	0	300
Eth6/10	0	0	0	0	30
	0	0	0	0	300
Eth6/11	0	0	0	0	30
	0	0	0	0	300
Eth6/12	0	0	0	0	30
	0	0	0	0	300
Eth6/13	0	0	0	0	30
	0	0	0	0	300
Eth6/14	0	0	0	0	30
	0	0	0	0	300
Eth6/15	0	0	0	0	30
	0	0	0	0	300
Eth6/16	0	0	0	0	30
	0	0	0	0	300
Eth6/17	0	0	0	0	30
	0	0	0	0	300
Eth6/18	0	0	0	0	30
	0	0	0	0	300
Eth6/19	0	0	0	0	30
	0	0	0	0	300
Eth6/20	0	0	0	0	30
	0	0	0	0	300
Eth6/21	0	0	0	0	30
	0	0	0	0	300
Eth6/22	0	0	0	0	30
	0	0	0	0	300
Eth6/23	0	0	0	0	30
	0	0	0	0	300
Eth6/24	0	0	0	0	30
	0	0	0	0	300
Eth6/25	0	0	0	0	30
	0	0	0	0	300
Eth6/26	0	0	0	0	30
	0	0	0	0	300
Eth6/27	0	0	0	0	30
	0	0	0	0	300
Eth6/28	0	0	0	0	30
	0	0	0	0	300
Eth6/29	0	0	0	0	30
	0	0	0	0	300
Eth6/30	0	0	0	0	30
	0	0	0	0	300
Eth6/31	0	0	0	0	30
	0	0	0	0	300
Eth6/32	0	0	0	0	30
	0	0	0	0	300

```
switch# show interface counters brief load-interval 2
```

Interface	Input Rate (avg)		Output Rate (avg)		Rate averaging interval (seconds)
	Rate MB/s	Total Frames	Rate MB/s	Total Frames	
Eth6/1	0	0	0	0	300
Eth6/2	0	0	0	0	300
Eth6/3	0	0	0	0	300
Eth6/4	0	0	0	0	300
Eth6/5	0	0	0	0	300
Eth6/6	0	0	0	0	300
Eth6/7	0	0	0	0	300
Eth6/8	0	0	0	0	300
Eth6/9	0	0	0	0	300
Eth6/10	0	0	0	0	300
Eth6/11	0	0	0	0	300
Eth6/12	0	0	0	0	300
Eth6/13	0	0	0	0	300
Eth6/14	0	0	0	0	300
Eth6/15	0	0	0	0	300
Eth6/16	0	0	0	0	300
Eth6/17	0	0	0	0	300
Eth6/18	0	0	0	0	300
Eth6/19	0	0	0	0	300
Eth6/20	0	0	0	0	300
Eth6/21	0	0	0	0	300
Eth6/22	0	0	0	0	300
Eth6/23	0	0	0	0	300
Eth6/24	0	0	0	0	300
Eth6/25	0	0	0	0	300
Eth6/26	0	0	0	0	300
Eth6/27	0	0	0	0	300
Eth6/28	0	0	0	0	300
Eth6/29	0	0	0	0	300
Eth6/30	0	0	0	0	300
Eth6/31	0	0	0	0	300
Eth6/32	0	0	0	0	300

```
switch(config)# show interface e6/1 counters brief
```

Interface	Input Rate (avg)		Output Rate (avg)		Rate averaging interval (seconds)
	Rate MB/s	Total Frames	Rate MB/s	Total Frames	
Eth6/1	0	0	0	0	30
Eth6/1	0	0	0	0	300

```
switch(config)# show interval e6/1 counters brief load-interval 2
```

Interface	Input Rate (avg)		Output Rate (avg)		Rate averaging interval (seconds)
	Rate MB/s	Total Frames	Rate MB/s	Total Frames	
Eth6/1	0	0	0	0	300

Related Commands

Command	Description
clear counters interface	Clears the counters for all load intervals on the specified interfaces.

show interface counters errors

To display interface error counters, use the **show interface counters errors** command.

show interface [{**ethernet** *slot/port* | **port-channel** *channel-number*}]**counterserrors**

Syntax Description	Parameter	Description
	ethernet	(Optional) Specifies the slot and port of the Ethernet interface that you want to display.
	<i>slot/port</i>	(Optional) Slot number and port number for the Ethernet interface. The range is from 1 to 253.
	port-channel	(Optional) Specifies the port-channel number of the port-channel interface that you want to display.
	<i>channel-number</i>	(Optional) Channel number. The range is from 1 to 4096.

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	4.0	This command was introduced.

Usage Guidelines Use the **show interface counters errors** command to display interface error counters. If you do not specify an interface, this command displays information about all Layer 2 interfaces.

This command does not require a license.

Examples

This example shows how to display the interface error counters:

```
switch# show interface counters errors
-----
Port          Align-Err    FCS-Err     Xmit-Err    Rcv-Err     UnderSize  OutDiscards
-----
mgmt0         --          --          --          --          --          --
Eth2/1        0           0           0           0           0           0
Eth2/2        0           0           0           0           0           0
Eth2/3        0           0           0           0           0           0
Eth2/4        0           0           0           0           0           0
Eth2/5        0           0           0           0           0           0
Eth2/6        0           0           0           0           0           0
Eth2/7        0           0           0           0           0           0
Eth2/8        0           0           0           0           0           0
Eth2/9        0           0           0           0           0           0
Eth2/10       0           0           0           0           0           0
Eth2/11       0           0           0           0           0           0
Eth2/12       0           0           0           0           0           0
Eth2/13       0           0           0           0           0           0
Eth2/14       0           0           0           0           0           0
Eth2/15       0           0           0           0           0           0
Eth2/16       0           0           0           0           0           0
Eth2/17       0           0           0           0           0           0
```

show interface counters errors

Eth2/18	0	0	0	0	0	0
Eth2/19	0	0	0	0	0	0
Eth2/20	0	0	0	0	0	0
Eth2/21	0	0	0	0	0	0
Eth2/22	0	0	0	0	0	0
Eth2/23	0	0	0	0	0	0
Eth2/24	0	0	0	0	0	0
Eth2/25	0	0	0	0	0	0
Eth2/26	0	0	0	0	0	0
Eth2/27	0	0	0	0	0	0
Eth2/28	0	0	0	0	0	0
Eth2/29	0	0	0	0	0	0
Eth2/30	0	0	0	0	0	0
Eth2/31	0	0	0	0	0	0
Eth2/32	0	0	0	0	0	0
Eth2/33	0	0	0	0	0	0
Eth2/34	0	0	0	0	0	0
Eth2/35	0	0	0	0	0	0
Eth2/36	0	0	0	0	0	0
Eth2/37	0	0	0	0	0	0
Eth2/38	0	0	0	0	0	0
Eth2/39	0	0	0	0	0	0
Eth2/40	0	0	0	0	0	0
Eth2/41	0	0	0	0	0	0
Eth2/42	0	0	0	0	0	0
Eth2/43	0	0	0	0	0	0
Eth2/44	0	0	0	0	0	0
Eth2/45	0	0	0	0	0	0
Eth2/46	0	0	0	0	0	0
Eth2/47	0	0	0	0	0	0
Eth2/48	0	0	0	0	0	0

Port	Single-Col	Multi-Col	Late-Col	Exces-Col	Carri-Sen	Runts
mgmt0	--	--	--	--	--	--
Eth2/1	0	0	0	0	0	0
Eth2/2	0	0	0	0	0	0
Eth2/3	0	0	0	0	0	0
Eth2/4	0	0	0	0	0	0
Eth2/5	0	0	0	0	0	0
Eth2/6	0	0	0	0	0	0
Eth2/7	0	0	0	0	0	0
Eth2/8	0	0	0	0	0	0
Eth2/9	0	0	0	0	0	0
Eth2/10	0	0	0	0	0	0
Eth2/11	0	0	0	0	0	0
Eth2/12	0	0	0	0	0	0
Eth2/13	0	0	0	0	0	0
Eth2/14	0	0	0	0	0	0
Eth2/15	0	0	0	0	0	0
Eth2/16	0	0	0	0	0	0
Eth2/17	0	0	0	0	0	0
Eth2/18	0	0	0	0	0	0
Eth2/19	0	0	0	0	0	0
Eth2/20	0	0	0	0	0	0
Eth2/21	0	0	0	0	0	0
Eth2/22	0	0	0	0	0	0
Eth2/23	0	0	0	0	0	0
Eth2/24	0	0	0	0	0	0
Eth2/25	0	0	0	0	0	0
Eth2/26	0	0	0	0	0	0
Eth2/27	0	0	0	0	0	0
Eth2/28	0	0	0	0	0	0
Eth2/29	0	0	0	0	0	0

Eth2/30	0	0	0	0	0	0
Eth2/31	0	0	0	0	0	0
Eth2/32	0	0	0	0	0	0
Eth2/33	0	0	0	0	0	0
Eth2/34	0	0	0	0	0	0
Eth2/35	0	0	0	0	0	0
Eth2/36	0	0	0	0	0	0
Eth2/37	0	0	0	0	0	0
Eth2/38	0	0	0	0	0	0
Eth2/39	0	0	0	0	0	0
Eth2/40	0	0	0	0	0	0
Eth2/41	0	0	0	0	0	0
Eth2/42	0	0	0	0	0	0
Eth2/43	0	0	0	0	0	0
Eth2/44	0	0	0	0	0	0
Eth2/45	0	0	0	0	0	0
Eth2/46	0	0	0	0	0	0
Eth2/47	0	0	0	0	0	0
Eth2/48	0	0	0	0	0	0

Port	Giants	SQETest-Err	Deferred-Tx	IntMacTx-Er	IntMacRx-Er	Symbol-Err

mgmt0	--	--	--	--	--	--
Eth2/1	0	--	0	0	0	0
Eth2/2	0	--	0	0	0	0
Eth2/3	0	--	0	0	0	0
Eth2/4	0	--	0	0	0	0
Eth2/5	0	--	0	0	0	0
Eth2/6	0	--	0	0	0	0
Eth2/7	0	--	0	0	0	0
Eth2/8	0	--	0	0	0	0
Eth2/9	0	--	0	0	0	0
Eth2/10	0	--	0	0	0	0
Eth2/11	0	--	0	0	0	0
Eth2/12	0	--	0	0	0	0
Eth2/13	0	--	0	0	0	0
Eth2/14	0	--	0	0	0	0
Eth2/15	0	--	0	0	0	0
Eth2/16	0	--	0	0	0	0
Eth2/17	0	--	0	0	0	0
Eth2/18	0	--	0	0	0	0
Eth2/19	0	--	0	0	0	0
Eth2/20	0	--	0	0	0	0
Eth2/21	0	--	0	0	0	0
Eth2/22	0	--	0	0	0	0
Eth2/23	0	--	0	0	0	0
Eth2/24	0	--	0	0	0	0
Eth2/25	0	--	0	0	0	0
Eth2/26	0	--	0	0	0	0
Eth2/27	0	--	0	0	0	0
Eth2/28	0	--	0	0	0	0
Eth2/29	0	--	0	0	0	0
Eth2/30	0	--	0	0	0	0
Eth2/31	0	--	0	0	0	0
Eth2/32	0	--	0	0	0	0
Eth2/33	0	--	0	0	0	0
Eth2/34	0	--	0	0	0	0
Eth2/35	0	--	0	0	0	0
Eth2/36	0	--	0	0	0	0
Eth2/37	0	--	0	0	0	0
Eth2/38	0	--	0	0	0	0
Eth2/39	0	--	0	0	0	0
Eth2/40	0	--	0	0	0	0
Eth2/41	0	--	0	0	0	0

show interface counters errors

```

Eth2/42          0          --          0          0          0          0
Eth2/43          0          --          0          0          0          0
Eth2/44          0          --          0          0          0          0
Eth2/45          0          --          0          0          0          0
Eth2/46          0          --          0          0          0          0
Eth2/47          0          --          0          0          0          0
Eth2/48          0          --          0          0          0          0

```

Related Commands

Command	Description
clear counters interface	Clears the counters for the specified interfaces.

show interface counters storm-control

To display interface storm control discard counters, use the **show interface counters storm-control** command.

show interface [{**ethernet** *slot/port* | **port-channel** *channel-number*}]**countersstorm-control**

Syntax Description	Parameter	Description
	ethernet	(Optional) Specifies the slot and port of the Ethernet interface that you want to display.
	<i>slot/port</i>	(Optional) Slot number and port number for the Ethernet interface. The range is from 1 to 253.
	port-channel	(Optional) Specifies the port-channel number of the port-channel interface that you want to display.
	<i>channel-number</i>	(Optional) Channel number. The range is from 1 to 4096.

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	4.0	This command was introduced.

Usage Guidelines Use the **show interface counters storm-control** command to display interface storm control discard counters. If you do not specify an interface, this command displays information about all Layer 2 interfaces.

This command does not require a license.

Examples

This example shows how to display the interface storm control discard counters:

```
switch# show interface counters storm-control
-----
Port          UcastSupp %    McastSupp %    BcastSupp %    TotalSuppDiscards
-----
Eth2/1        100.00         100.00         100.00         0
Eth2/2        100.00         100.00         100.00         0
Eth2/3        100.00         100.00         100.00         0
Eth2/4        100.00         100.00         100.00         0
Eth2/5        100.00         100.00         100.00         0
Eth2/6        100.00         100.00         100.00         0
Eth2/7        100.00         100.00         100.00         0
Eth2/8        100.00         100.00         100.00         0
Eth2/9        100.00         100.00         100.00         0
Eth2/10       100.00         100.00         100.00         0
Eth2/11       100.00         100.00         100.00         0
Eth2/12       100.00         100.00         100.00         0
Eth2/13       100.00         100.00         100.00         0
Eth2/14       100.00         100.00         100.00         0
Eth2/15       100.00         100.00         100.00         0
Eth2/16       100.00         100.00         100.00         0
Eth2/17       100.00         100.00         100.00         0
Eth2/18       100.00         100.00         100.00         0
```

show interface counters storm-control

```

Eth2/19      100.00      100.00      100.00      0
Eth2/20      100.00      100.00      100.00      0
Eth2/21      100.00      100.00      100.00      0
Eth2/22      100.00      100.00      100.00      0
Eth2/23      100.00      100.00      100.00      0
Eth2/24      100.00      100.00      100.00      0
Eth2/25      100.00      100.00      100.00      0
Eth2/26      100.00      100.00      100.00      0
Eth2/27      100.00      100.00      100.00      0
Eth2/28      100.00      100.00      100.00      0
Eth2/29      100.00      100.00      100.00      0
Eth2/30      100.00      100.00      100.00      0
Eth2/31      100.00      100.00      100.00      0
Eth2/32      100.00      100.00      100.00      0
Eth2/33      100.00      100.00      100.00      0
Eth2/34      100.00      100.00      100.00      0
Eth2/35      100.00      100.00      100.00      0
Eth2/36      100.00      100.00      100.00      0
Eth2/37      100.00      100.00      100.00      0
Eth2/38      100.00      100.00      100.00      0
Eth2/39      100.00      100.00      100.00      0
Eth2/40      100.00      100.00      100.00      0
Eth2/41      100.00      100.00      100.00      0
Eth2/42      100.00      100.00      100.00      0
Eth2/43      100.00      100.00      100.00      0
Eth2/44      100.00      100.00      100.00      0
Eth2/45      100.00      100.00      100.00      0
Eth2/46      100.00      100.00      100.00      0
Eth2/47      100.00      100.00      100.00      0
Eth2/48      100.00      100.00      100.00      0

```

Related Commands

Command	Description
clear counters interface	Clears the counters for the specified interfaces.

show interface counters trunk

To display the counters for Layer 2 switch port trunk interfaces, use the **show interface counters trunk** command.

show interface [{ethernet}slot/port]counterstrunk

Syntax Description	ethernet	(Optional) Specifies the slot and port of the Ethernet interface that you want to display.
	slot/port	(Optional) Slot number and port number for the Ethernet interface. The range is from 1 to 253.

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	4.0	This command was introduced.

Usage Guidelines The device supports only IEEE 802.1Q encapsulation. This command also displays the counters for trunk port channels.

This command does not require a license.

Examples

This example shows how to display the counters for a trunk interface. This display shows the frames transmitted and received through the trunk interface, as well as the number of frames with the wrong trunk encapsulation:

```
switch# show interface ethernet 2/9 counters trunk
-----
Port           TrunkFramesTx  TrunkFramesRx  WrongEncap
-----
Ethernet2/9           0              0              0
```

Related Commands	Command	Description
	clear counters interface	Clears the counters for the specified interfaces.

show interface debounce

To display the debounce time information about the interface, use the **show interface debounce** command.

show interface [{**ethernet** *slot/port* | **port-channel** *channel-number*}]**debounce**

Syntax Description

ethernet	(Optional) Specifies the slot and port of the Ethernet interface that you want to display.
<i>slot/port</i>	(Optional) Slot number and port number for the Ethernet interface. The range is from 1 to 253.
port-channel	(Optional) Specifies the port-channel number of the port-channel interface that you want to display.
<i>channel-number</i>	(Optional) Channel number. The range is from 1 to 4096.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **show interface debounce** command to display debounce time information about the interface. If you do not specify an interface, this command displays information about all Layer 2 interfaces.

This command does not require a license.

Examples

This example shows how to display debounce time information about the interface:

```
switch# show interface debounce
-----
Port           Debounce time  Value (ms)
-----
Eth2/1         enable         100
Eth2/2         enable         100
Eth2/3         enable         100
Eth2/4         enable         100
Eth2/5         enable         100
Eth2/6         enable         100
Eth2/7         enable         100
Eth2/8         enable         100
Eth2/9         enable         100
Eth2/10        enable         100
Eth2/11        enable         100
Eth2/12        enable         100
Eth2/13        enable         100
Eth2/14        enable         100
Eth2/15        enable         100
Eth2/16        enable         100
Eth2/17        enable         100
Eth2/18        enable         100
```

```

Eth2/19      enable      100
Eth2/20      enable      100
Eth2/21      enable      100
Eth2/22      enable      100
Eth2/23      enable      100
Eth2/24      enable      100
Eth2/25      enable      100
Eth2/26      enable      100
Eth2/27      enable      100
Eth2/28      enable      100
Eth2/29      enable      100
Eth2/30      enable      100
Eth2/31      enable      100
Eth2/32      enable      100
Eth2/33      enable      100
Eth2/34      enable      100
Eth2/35      enable      100
Eth2/36      enable      100
Eth2/37      enable      100
Eth2/38      enable      100
Eth2/39      enable      100
Eth2/40      enable      100
Eth2/41      enable      100
Eth2/42      enable      100
Eth2/43      enable      100
Eth2/44      enable      100
Eth2/45      enable      100
Eth2/46      enable      100
Eth2/47      enable      100
Eth2/48      enable      100

```

Related Commands

Command	Description
link debounce time	Enables the debounce timer for Ethernet ports.

show interface description

To display a description about the interface, use the **show interface description** command.

show interface description

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Any command mode

Release	Modification
4.0	This command was introduced.

Usage Guidelines Use the show interface description command to display the interface description.
This command does not require a license.

Examples This example shows how to display a description of the interface:

```
switch# show interface description
-----
Interface                Description
-----
mgmt0                    --
-----
Port          Type    Speed  Description
-----
Eth2/1        eth     1000   --
Eth2/2        eth     1000   --
Eth2/3        eth     1000   --
Eth2/4        eth     1000   --
Eth2/5        eth     1000   --
Eth2/6        eth     1000   --
Eth2/7        eth     1000   server2
Eth2/8        eth     1000   --
Eth2/9        eth     1000   --
Eth2/10       eth     1000   ethernet slot 2 port 10
Eth2/11       eth     1000   --
Eth2/12       eth     1000   --
Eth2/13       eth     1000   --
Eth2/14       eth     1000   --
Eth2/15       eth     1000   --
Eth2/16       eth     1000   --
Eth2/17       eth     1000   --
Eth2/18       eth     1000   --
Eth2/19       eth     1000   --
Eth2/20       eth     1000   --
Eth2/21       eth     1000   --
Eth2/22       eth     1000   --
Eth2/23       eth     1000   --
Eth2/24       eth     1000   --
Eth2/25       eth     1000   --
```



```
Eth2/26      eth    1000  --
Eth2/27      eth    1000  --
Eth2/28      eth    1000  --
Eth2/29      eth    1000  --
Eth2/30      eth    1000  --
Eth2/31      eth    1000  --
Eth2/32      eth    1000  --
Eth2/33      eth    1000  --
...<additional lines truncated>
```

Related Commands

Command	Description
description	Provides textual interface descriptions for interfaces.

show interface ethernet

To display information about the Ethernet interface, use the **show interface ethernet** command.

```
show interface ethernet slot/port [ { brief | cable-diagnostics-tdr | capabilities | counters { brief | detailed | errors | snmp | storm-control | trunk } | debounce | description | fcoe | flowcontrol | mac-address | status { err-disabled | err-vlans } | switchport | transceiver | trunk } ]
```

Syntax Description

<i>slot/port</i>	Slot number and port number for the Ethernet interface. The range is from 1 to 253.
brief	(Optional) Displays brief information about the interface.
cable-diagnostics-tdr	(Optional) Displays information about the time domain reflectometer (TDR) test.
capabilities	(Optional) Displays interface capabilities.
counters	Displays the counters.
brief	Displays information about the counters in brief.
detailed	Displays only nonzero counters.
errors	Displays error counters in the interface.
snmp	Displays SNMP MIB values.
storm-control	Displays storm-control counters.
trunk	Displays trunk counters.
debounce	(Optional) Displays the debounce time of the interface.
description	(Optional) Displays the interface description.
fcoe	(Optional) Displays the Fibre Channel over Ethernet (FCoE) information of the interface.
flowcontrol	(Optional) Displays the flow-control information.
mac-address	(Optional) Displays the MAC address.
status	(Optional) Displays the link status of the interface.
err-disabled	Displays the error-disabled state of the interface.
err-vlans	Displays VLAN errors in the interface.
switchport	(Optional) Displays switch-port information.
transceiver	(Optional) Displays the transceiver information.
trunk	(Optional) Displays interface trunk information.

Command Default None

Command Modes Any command mode

Release	Modification
5.1(1)	Added the brief, cable-diagnostics-tdr, capabilities, debounce, description, detailed, errors, err-disabled, err-vlans, fcoe, flowcontrol, mac-address, snmp, storm-control, status, switchport, transceiver, and trunk keywords.
4.0	This command was introduced.

Usage Guidelines Use the **show interface ethernet** command to display information about the Ethernet interface. This command does not require a license.

Examples This example shows how to display information about the Ethernet interface:

```
switch# show interface ethernet 2/5
Ethernet2/5 is down (Administratively down)
  Hardware: 10/100/1000 Ethernet, address: 0018.bad8.3ffd (bia 0019.076c.4db0)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA
  auto-duplex, auto-speed
  Beacon is turned off
  Auto-Negotiation is turned on
  Input flow-control is off, output flow-control is off
  Auto-mdix is turned on
  Switchport monitor is off
  Last clearing of "show interface" counters never
  1 minute input rate 0 bits/sec, 0 packets/sec
  1 minute output rate 0 bits/sec, 0 packets/sec
  L3 in Switched:
    ucast: 0 pkts, 0 bytes - mcast: 0 pkts, 0 bytes
  L3 out Switched:
    ucast: 0 pkts, 0 bytes - mcast: 0 pkts, 0 bytes
  Rx
    0 input packets 0 unicast packets 0 multicast packets
    0 broadcast packets 0 jumbo packets 0 storm suppression packets
    0 bytes
  Tx
    0 output packets 0 multicast packets
    0 broadcast packets 0 jumbo packets
    0 bytes
    0 input error 0 short frame 0 watchdog
    0 no buffer 0 runt 0 CRC 0 ecc
    0 overrun 0 underrun 0 ignored 0 bad etype drop
    0 bad proto drop 0 if down drop 0 input with dribble
    0 input discard
    0 output error 0 collision 0 deferred
    0 late collision 0 lost carrier 0 no carrier
    0 babble
    0 Rx pause 0 Tx pause
  0 interface resets
```

Related Commands

Command	Description
interface	Enters the interface configuration mode and configures the types and identities of interfaces.

show interface flowcontrol

To display the flow-control configuration for all or a specified interface, use the **show interface flowcontrol** command.

show interface flowcontrol [{fex | port-channel *channel-number*}] flowcontrol

Syntax Description	Parameter	Description
	fex	(Optional) Displays the Fabric Extender interface that you want to display. the range is from 100 to 199.
	port-channel <i>channel-number</i>	(Optional) Displays the port-channel number of the port-channel interface that you want to display. The range is from 1 to 4096.
	flowcontrol	(Optional) Displays the interface flowcontrol information.

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	4.0	This command was introduced.
	5.1	The fex keyword was added.

Usage Guidelines Use the **show interface flowcontrol** command to display information about the interface flow control. If you do not specify an interface, this command displays information about all Layer 2 interfaces.

This command does not require a license.

Examples

This example shows how to display the interface flow-control information:

```
switch# show interface flowcontrol
-----
Port          Send FlowControl  Receive FlowControl  RxPause TxPause
              admin    oper    admin    oper
-----
Eth2/1        off      off      off      off      0      0
Eth2/2        off      off      off      off      0      0
Eth2/3        off      off      off      off      0      0
Eth2/4        off      off      off      off      0      0
Eth2/5        off      off      off      off      0      0
Eth2/6        off      off      off      off      0      0
Eth2/7        off      off      off      off      0      0
Eth2/8        off      off      off      off      0      0
Eth2/9        off      off      off      off      0      0
Eth2/10       off      off      off      off      0      0
Eth2/11       off      off      off      off      0      0
Eth2/12       off      off      off      off      0      0
Eth2/13       off      off      off      off      0      0
Eth2/14       off      off      off      off      0      0
Eth2/15       off      off      off      off      0      0
Eth2/16       off      off      off      off      0      0
```

show interface flowcontrol

```

Eth2/17    off    off    off    off    0      0
Eth2/18    off    off    off    off    0      0
Eth2/19    off    off    off    off    0      0
Eth2/20    off    off    off    off    0      0
Eth2/21    off    off    off    off    0      0
Eth2/22    off    off    off    off    0      0
Eth2/23    off    off    off    off    0      0
Eth2/24    off    off    off    off    0      0
Eth2/25    off    off    off    off    0      0
Eth2/26    off    off    off    off    0      0
Eth2/27    off    off    off    off    0      0
Eth2/28    off    off    off    off    0      0
Eth2/29    off    off    off    off    0      0
Eth2/30    off    off    off    off    0      0
Eth2/31    off    off    off    off    0      0
Eth2/32    off    off    off    off    0      0
Eth2/33    off    off    off    off    0      0
Eth2/34    off    off    off    off    0      0
Eth2/35    off    off    off    off    0      0
Eth2/36    off    off    off    off    0      0
Eth2/37    off    off    off    off    0      0
Eth2/38    off    off    off    off    0      0
Eth2/39    off    off    off    off    0      0
Eth2/40    off    off    off    off    0      0
Eth2/41    off    off    off    off    0      0
Eth2/42    off    off    off    off    0      0
Eth2/43    off    off    off    off    0      0
Eth2/44    off    off    off    off    0      0
Eth2/45    off    off    off    off    0      0
Eth2/46    off    off    off    off    0      0
Eth2/47    off    off    off    off    0      0
Eth2/48    off    off    off    off    0      0

```

Related Commands

Command	Description
flowcontrol	Enables or disables the ability of the Ethernet port to send and receive flow-control pause frames.

show interface mgmt

To display the management interface information, use the **show interface mgmt** command.

show interface mgmt *number* [{**brief** | **counters** [{**detailed** | **errors** [**snmp**]}] | **description** | **status**}]

Syntax Description		
	<i>number</i>	Information about the management interface number. The valid value is 0 .
	brief	(Optional) Displays brief information about the management interface .
	counters	(Optional) Displays the counters for the management interface .
	detailed	(Optional) Displays detailed information about the counters for the management interface .
	errors	(Optional) Displays the errors for the management interface .
	snmp	(Optional) Displays the SNMP errors for the management interface .
	description	(Optional) Displays the description of the management interface .
	status	(Optional) Displays the status of the management interface .

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	4.0	This command was introduced.

Usage Guidelines Use the **show interface mgmt** *number* command to display information about the management interface. This command does not require a license.

Examples This example shows how to display the management interface information:

```
switch# show interface mgmt0
mgmt0 is up
  Hardware: GigabitEthernet, address: 0019.076c.1a78 (bia 0019.076c.1a78)
  Internet Address is 172.28.231.193/23
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA
  full-duplex, 1000 Mb/s
  Auto-Negotiation is turned on
  1 minute input rate 6446522 bits/sec, 78642 packets/sec
  1 minute output rate 1965455 bits/sec, 20644 packets/sec
  Rx
    78681 input packets 15607 unicast packets 20178 multicast packets
    42896 broadcast packets 24189392 bytes
  Tx
    20647 output packets 20377 unicast packets 246 multicast packets
    24 broadcast packets 7370904 bytes
```

Related Commands

Command	Description
interface	Enters the interface configuration mode and configures the types and identities of interfaces.

show interface port-channel

To display descriptive information about port channels, use the **show interface port-channel** command.

show interface port-channel *channel-number* [{**brief** | **description** | **flowcontrol** | **status** | **switchport** | **trunk**}]

Syntax Description	
<i>channel-number</i>	Number of the port-channel group. The range is from 1 to 4096.
brief	(Optional) Specifies the summary information for specified port channels.
description	(Optional) Specifies the description of specified port channels.
flowcontrol	(Optional) Specifies information about the flow-control status control for specified port channels and the statistics on received and transmitted flow-control pause packets.
status	(Optional) Specifies information about the status for specified port channels.
switchport	(Optional) Specifies information for specified Layer 2 port channels including access and trunk modes.
trunk	(Optional) Specifies information for specified Layer 2 port channels on the trunk mode.

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	4.2(1)	Display of configured static MAC address for Layer 3 port channels was added.
	4.0	This command was introduced.

Usage Guidelines To display more statistics for the specified port channels, use the **show interface port-channel counters** command.

This command does not require a license.

Examples

This example shows how to display information for a specific port channel. This example displays statistical information gathered on the port channel at 1-minute intervals:

```
switch# show interface port-channel 101
port-channel101 is up
admin state is up,
  Hardware: Port-Channel, address: 0026.9825.58e4 (bia 0026.9825.58e4)
  MTU 9216 bytes, BW 20000000 Kbit, DLY 10 usec
  reliability 255/255, txload 16/255, rxload 16/255
  Encapsulation ARPA, medium is broadcast
  Port mode is fex-fabric
  full-duplex, 10 Gb/s
  Input flow-control is off, output flow-control is off
```

show interface port-channel

```

Auto-mdix is turned off
Switchport monitor is off
EtherType is 0x8100
Members in this channel: Eth7/1, Eth8/1
Last clearing of "show interface" counters never
1 interface resets
30 seconds input rate 1264864848 bits/sec, 1736043 packets/sec
30 seconds output rate 1264870712 bits/sec, 1736074 packets/sec
Load-Interval #2: 5 minute (300 seconds)
  input rate 1.25 Gbps, 1.72 Mpps; output rate 1.25 Gbps, 1.72 Mpps
RX
  733914 unicast packets  382406768498 multicast packets  11476533567 broadcast packets
  393884035979 input packets  36031214919080 bytes
  0 jumbo packets  0 storm suppression packets
  0 runts  0 giants  0 CRC  0 no buffer
  0 input error  0 short frame  0 overrun  0 underrun  0 ignored
  0 watchdog  0 bad etype drop  0 bad proto drop  0 if down drop
  0 input with dribble  0 input discard
  62339596 Rx pause
TX
  1019601 unicast packets  382406766702 multicast packets  11476533707 broadcast packets
  393884320010 output packets  36030918130654 bytes
  0 jumbo packets
  0 output error  0 collision  0 deferred  0 late collision
  0 lost carrier  0 no carrier  0 babble  0 output discard
  0 Tx pause

```

This example shows how to display a brief description for a specific port channel, including the mode for the port channel, the status, speed, and protocol:

```

switch# show interface port-channel 5 brief
-----
Port-channel VLAN  Type Mode    Status  Reason                               Speed  Protocol
Interface
-----
                eth  access down    No operational members             auto(D)  lacp

```

This example shows how to display the description for a specific port channel:

```

switch# show interface port-channel 5 description
-----
Interface          Description
-----
port-channel5      test

```

This example shows how to display the flow-control information for a specific port channel:

```

switch# show interface port-channel 50 flowcontrol
-----
Port      Send FlowControl  Receive FlowControl  RxPause  TxPause
         admin   oper    admin   oper
-----
Po50     off    off     off     off         0        0

```

The **oper** display for the *show interface port-channel flowcontrol* command shows as on if one member of the port channel is set to on for flow control and all the of the members and the entire port channel is set to on for flow control.

This example shows how to display the status of a specific port channel:

```

switch# show interface port-channel 5 status

```

```

-----
Port          Name          Status  Vlan    Duplex  Speed  Type
-----
              test          down    1       auto    auto   --
    
```

This example shows how to display information for a specific Layer 2 port channel:

```

switch#
show interface port-channel 50 switchport
Name: port-channel50
  Switchport: Enabled
  Switchport Monitor: Not enabled
  Operational Mode: trunk
  Access Mode VLAN: 1 (default)
  Trunking Native Mode VLAN: 1 (default)
  Trunking VLANs Enabled: 1-3967,4048-4093
  Administrative private-vlan primary host-association: none
  Administrative private-vlan secondary host-association: none
  Administrative private-vlan primary mapping: none
  Administrative private-vlan secondary mapping: none
  Administrative private-vlan trunk native VLAN: none
  Administrative private-vlan trunk encapsulation: dot1q
  Administrative private-vlan trunk normal VLANs: none
  Administrative private-vlan trunk private VLANs: none
  Operational private-vlan: none
    
```

This command displays information for Layer 2 port channels in both the access and trunk modes.

When you use this command for a routed port channel, the device returns the following message:

```

Name: port-channel20
  Switchport: Disabled
    
```

This example shows how to display information for a specific Layer 2 port channel that is in trunk mode:

```

switch# show interface port-channel 5 trunk
switch# show interface port-channel 50 trunk
port-channel50 is down (No operational members)
  Hardware is Ethernet, address is 0000.0000.0000
  MTU 1500 bytes, BW 100000 Kbit, DLY 10 usec
  Port mode is access
  Speed is auto-speed
  Duplex mode is auto
  Beacon is turned off
  Receive flow-control is off, Send flow-control is off
  Rate mode is dedicated
  Members in this channel: Eth2/10
  Native Vlan: 1
  Allowed Vlans: 1-3967,4048-4093
    
```

This command displays information for only Layer 2 port channels in the trunk modes; you cannot display information about Layer 2 port channels in the access mode with this command.

Related Commands

Command	Description
show interface port-channel counters	Displays the statistics for channel groups.
show port-channel summary	Displays summary information for all channel groups.

show interface port-channel counters

To display information about port-channel statistics, use the **show interface port-channel counters** command.

```
show interface port-channel channel-number counters [{brief | detailed [{all | snmp}] | errors
[snmp] | trunk}]
```

Syntax Description

<i>channel-number</i>	Number of the port-channel group. The range is from 1 to 4096.
brief	(Optional) Specifies the rate MB/s and total frames for specified port channels.
detailed	(Optional) Specifies the n onzero counters for specified port channels.
all	(Optional) Specifies the c ounters for specified port channels.
snmp	(Optional) Specifies the SNMP MIB values for specified port channels.
errors	(Optional) Specifies the interface error counters for specified port channels.
trunk	(Optional) Specifies the i nterface trunk counters for specified port channels.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

This command displays statistics for all port channels including the Link Aggregation Control Protocol (LACP)-enabled port channels and those port channels that are not associated with an aggregation protocol.

This command does not require a license.

Examples

This example shows how to display the counters for a specific port channel. This example display shows the transmitted and received unicast and multicast packets:

```
switch# show interface
port-channel 2
counters
Port          InOctets   InUcastPkts  InMcastPkts  InBcastPkts
Po2           6007       1             31            1
Port          OutOctets  OutUcastPkts  OutMcastPkts  OutBcastPkts
Po2           4428       1             25            1
```

This example shows how to display the brief counters for a specific port channel. This display shows the transmitted and received rate and total frames:

```
switch# show interface port-channel 20 counters brief
-----
Interface          Input (rate is 1 min avg)  Output (rate is 1 min avg)
```

	Rate MB/s	Total Frames	Rate MB/s	Total Frames
port-channel20	0	0	0	0

This example shows how to display all the detailed counters for a specific port channel:

```
switch# show interface port-channel 20 counters detailed all
port-channel20
 64 bit counters:
 0. rxHCTotalPkts = 0
 1. txHCTotalPks = 0
 2. rxHCUnicastPkts = 0
 3. txHCUnicastPkts = 0
 4. rxHCMulticastPkts = 0
 5. txHCMulticastPkts = 0
 6. rxHCBroadcastPkts = 0
 7. txHCBroadcastPkts = 0
 8. rxHCOctets = 0
 9. txHCOctets = 0
10. rxTxHCPkts64Octets = 0
11. rxTxHCPkts65to127Octets = 0
12. rxTxHCPkts128to255Octets = 0
13. rxTxHCPkts256to511Octets = 0
14. rxTxHCPkts512to1023Octets = 0
15. rxTxHCPkts1024to1518Octets = 0
16. rxTxHCPkts1519to1548Octets = 0
17. rxHCTrunkFrames = 0
18. txHCTrunkFrames = 0
19. rxHCDropEvents = 0
All Port Counters:
 0. InPackets = 0
 1. InOctets = 0
 2. InUcastPkts = 0
 3. InMcastPkts = 0
 4. InBcastPkts = 0
 5. InJumboPkts = 0
 6. StormSuppressPkts = 0
 7. OutPackets = 0
 8. OutOctets = 0
 9. OutUcastPkts = 0
10. OutMcastPkts = 0
11. OutBcastPkts = 0
12. OutJumboPkts = 0
13. rxHCPkts64Octets = 0
14. rxHCPkts65to127Octets = 0
15. rxHCPkts128to255Octets = 0
16. rxHCPkts256to511Octets = 0
17. rxHCpkts512to1023Octets = 0
18. rxHCpkts1024to1518Octets = 0
19. rxHCpkts1519to1548Octets = 0
20. txHCPkts64Octets = 0
21. txHCPkts65to127Octets = 0
22. txHCPkts128to255Octets = 0
23. txHCPkts256to511Octets = 0
24. txHCpkts512to1023Octets = 0
25. txHCpkts1024to1518Octets = 0
26. txHCpkts1519to1548Octets = 0
27. ShortFrames = 0
28. Collisions = 0
29. SingleCol = 0
30. MultiCol = 0
31. LateCol = 0
```

```

32.          ExcessiveCol = 0
33.          LostCarrier = 0
34.          NoCarrier = 0
35.          Runts = 0
36.          Giants = 0
37.          InErrors = 0
38.          OutErrors = 0
39.          InputDiscards = 0
40.          BadEtypeDrops = 0
41.          IfDownDrops = 0
42.          InUnknownProtos = 0
43.          txCRC = 0
44.          rxCRC = 0
45.          Symbol = 0
46.          txDropped = 0
47.          TrunkFramesTx = 0
48.          TrunkFramesRx = 0
49.          WrongEncap = 0
50.          Babbles = 0
51.          Watchdogs = 0
52.          ECC = 0
53.          Overruns = 0
54.          Underruns = 0
55.          Dribbles = 0
56.          Deferred = 0
57.          Jabbers = 0
58.          NoBuffer = 0
59.          Ignored = 0
60.          bpduOutLost = 0
61.          cos0OutLost = 0
62.          cos1OutLost = 0
63.          cos2OutLost = 0
64.          cos3OutLost = 0
65.          cos4OutLost = 0
66.          cos5OutLost = 0
67.          cos6OutLost = 0
68.          cos7OutLost = 0
69.          RxPause = 0
70.          TxPause = 0
71.          Resets = 0
72.          SQETest = 0
73.          InLayer3Routed = 0
74.          InLayer3RoutedOctets = 0
75.          OutLayer3Routed = 0
76.          OutLayer3RoutedOctets = 0
77.          OutLayer3Unicast = 0
78.          OutLayer3UnicastOctets = 0
79.          OutLayer3Multicast = 0
80.          OutLayer3MulticastOctets = 0
81.          InLayer3Unicast = 0
82.          InLayer3UnicastOctets = 0
83.          InLayer3Multicast = 0
84.          InLayer3MulticastOctets = 0
85.          InLayer3AverageOctets = 0
86.          InLayer3AveragePackets = 0
87.          OutLayer3AverageOctets = 0
88.          OutLayer3AveragePackets = 0

```

This example shows how to display the error counters for a specific port channel:

```

switch#
show interface port-channel 5 counters errors
-----
Port          Align-Err    FCS-Err    Xmit-Err    Rcv-Err    UnderSize  OutDiscards

```

```

-----
Po5          0          0          0          0          0          0
-----
Port      Single-Col  Multi-Col  Late-Col  Exces-Col  Carri-Sen  Runts
-----
Po5          0          0          0          0          0          0
-----
Port      Giants  SQETest-Err  Deferred-Tx  IntMacTx-Er  IntMacRx-Er  Symbol-Err
-----
          0          --          0          0          0          0
    
```

This example shows how to display information about the trunk interfaces for a specific port channel:

```

switch# show interface port-channel 5 counters trunk
-----
Port      TrunkFramesTx  TrunkFramesRx  WrongEncap
-----
port-channel5          0          0          0
    
```

Related Commands

Command	Description
clear counters	Clears the statistics for all interfaces that belong to a specific channel group.

show interface status

To display the interface line status, use the **show interface status** command.

show interface status [{**auto-column** | **down** | **err-disabled** | **err-vlans** | **error policy** [**detail**] | **inactive** | **module** *number* | **up**}]

Syntax Description

auto-column	(Optional) Displays complete interface status information, such as complete transceiver type and name. Note This option is hidden and not visible. To use this option, type show interface status auto-column .
down	(Optional) Displays the interface down state.
err-disabled	(Optional) Displays the interface error-disabled state.
err-vlans	(Optional) Displays the VLANs with errors.
error policy	(Optional) Displays the interfaces and VLANs that generated an error during policy programming.
detail	(Optional) Displays details of the interface that generated the error.
inactive	(Optional) Displays the interface inactive state.
module <i>number</i>	(Optional) Displays the module number. The range is from 1 to 18.
up	(Optional) Displays the interface up state.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.2(2)	Added the error policy keyword to the syntax description.
4.1(2)	The err-vlans parameter was added.
4.0	This command was introduced.

Usage Guidelines

Use the **show interface status** command to display the interface line status.

This command does not require a license.

Examples

This example shows how to view complete interface status information, such as complete transceiver type and name.


```
switch# show interface status auto-column
```

Port	Name	Status	Vlan	Duplex	Speed	Type
mgmt0	--	connected	routed	full	a-1000	--
Eth1/1	--	connected	routed	full	a-100G	QSFP-100G-LR4
Eth1/1.1	--	connected	routed	full	a-100G	QSFP-100G-LR4

This example shows how to display the interface status error policy details:

```
switch# configure terminal
switch# show interface status error policy detail
```

No.	Interface	Error Type	Time Stamp	Reason	VLAN
switch#					

This example shows how to display the interface status for a specific module:

```
switch# show interface status module 2
```

Port	Name	Status	Vlan	Duplex	Speed	Type
Eth2/1	--	down	routed	auto	auto	1000BaseT
Eth2/2	--	down	routed	auto	auto	1000BaseT
Eth2/3	--	down	routed	auto	auto	1000BaseT
Eth2/4	--	down	1	auto	auto	1000BaseT
Eth2/5	--	down	routed	auto	auto	1000BaseT
Eth2/6	--	down	1	auto	auto	1000BaseT
Eth2/7	server2	up	1	full	1000	1000BaseT
Eth2/8	--	down	routed	auto	auto	1000BaseT
Eth2/9	--	up	1	full	1000	1000BaseT
Eth2/10	ethernet slot 2 po	down	1	auto	auto	1000BaseT
Eth2/11	--	down	routed	auto	auto	1000BaseT
Eth2/12	--	down	routed	auto	auto	1000BaseT
Eth2/13	--	down	routed	auto	auto	1000BaseT
Eth2/14	--	down	routed	auto	auto	1000BaseT
Eth2/15	--	down	routed	auto	auto	1000BaseT
Eth2/16	--	down	routed	auto	auto	1000BaseT
Eth2/17	--	down	routed	auto	auto	1000BaseT
Eth2/18	--	down	routed	auto	auto	1000BaseT
Eth2/19	--	down	routed	auto	auto	1000BaseT
Eth2/20	--	down	routed	auto	auto	1000BaseT
Eth2/21	--	down	routed	auto	auto	1000BaseT
Eth2/22	--	down	routed	auto	auto	1000BaseT
Eth2/23	--	down	routed	auto	auto	1000BaseT
Eth2/24	--	down	routed	auto	auto	1000BaseT
Eth2/25	--	down	routed	auto	auto	1000BaseT
Eth2/26	--	down	routed	auto	auto	1000BaseT
Eth2/27	--	down	routed	auto	auto	1000BaseT
Eth2/28	--	down	routed	auto	auto	1000BaseT
Eth2/29	--	down	routed	auto	auto	1000BaseT
Eth2/30	--	down	routed	auto	auto	1000BaseT
Eth2/31	--	down	routed	auto	auto	1000BaseT
Eth2/32	--	down	routed	auto	auto	1000BaseT
Eth2/33	--	down	routed	auto	auto	1000BaseT
Eth2/34	--	down	routed	auto	auto	1000BaseT
Eth2/35	--	down	routed	auto	auto	1000BaseT
Eth2/36	--	down	routed	auto	auto	1000BaseT
Eth2/37	--	down	routed	auto	auto	1000BaseT
Eth2/38	--	down	routed	auto	auto	1000BaseT

show interface status

```

Eth2/39      --          down    routed   auto    auto    1000BaseT
Eth2/40      --          down    routed   auto    auto    1000BaseT
Eth2/41      --          down    routed   auto    auto    1000BaseT
Eth2/42      --          down    routed   auto    auto    1000BaseT
Eth2/43      --          down    routed   auto    auto    1000BaseT
Eth2/44      --          down    routed   auto    auto    1000BaseT
Eth2/45      --          down    routed   auto    auto    1000BaseT
Eth2/46      --          down    routed   auto    auto    1000BaseT
Eth2/47      --          down    routed   auto    auto    1000BaseT
Eth2/48      --          down    routed   auto    auto    1000BaseT

```

Related Commands

Command	Description
interface	Enters the interface configuration mode and configures the types and identities of interfaces.

show interface switchport

To display information about all the switch-port interfaces, use the **show interface switchport** command.

show interface [{*ethernet**type/slot* | *port-channel* *channel-number*}] **switchport**

Syntax Description	ethernet <i>type/slot</i>	(Optional) Type and number of the interface that you want to display .
	port-channel <i>channel-number</i>	(Optional) Specifies the port-channel number of the port-channel interface that you want to display. The range is from 1 to 4096.

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	4.2(1)	Information about private VLAN promiscuous trunk ports was added.
	4.0	This command was introduced.

Usage Guidelines If you do not specify an interface, this command displays information about all Layer 2 interfaces, including access, trunk, port-channel interfaces, and all private VLAN ports.

Use the **show interface counters** command to display statistics for the specified Layer 2 interface.

This command does not require a license.

Examples

This example shows how to display information for all Layer 2 interfaces:

```
switch# show interface switchport
Name: Ethernet2/5
  Switchport: Enabled
  Switchport Monitor: Not enabled
  Operational Mode: access
  Access Mode VLAN: 1 (default)
  Trunking Native Mode VLAN: 1 (default)
  Trunking VLANs Enabled: 1-3967,4048-4093
  Administrative private-vlan primary host-association: none
  Administrative private-vlan secondary host-association: none
  Administrative private-vlan primary mapping: none
  Administrative private-vlan secondary mapping: none
  Administrative private-vlan trunk native VLAN: none
  Administrative private-vlan trunk encapsulation: dot1q
  Administrative private-vlan trunk normal VLANs: none
  Administrative private-vlan trunk private VLANs: none
  Operational private-vlan: none
Name: Ethernet2/9
  Switchport: Enabled
  Switchport Monitor: Not enabled
  Operational Mode: trunk
  Access Mode VLAN: 1 (default)
  Trunking Native Mode VLAN: 1 (default)
  Trunking VLANs Enabled: 1-3967,4048-4093
```

show interface switchport

```

Administrative private-vlan primary host-association: none
Administrative private-vlan secondary host-association: none
Administrative private-vlan primary mapping: none
Administrative private-vlan secondary mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Name: port-channel5
Switchport: Enabled
Switchport Monitor: Not enabled
Operational Mode: access
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: 1-3967,4048-4093
Administrative private-vlan primary host-association: none
Administrative private-vlan secondary host-association: none
Administrative private-vlan primary mapping: none
Administrative private-vlan secondary mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none

```

Beginning with Cisco NX-OS Release 4.2(1), you can display information on private VLAN promiscuous trunk ports on Cisco Nexus 7000 Series devices. This example shows how to display information for those interfaces:

```

switch# show interface switchport
Name: Ethernet7/4
Switchport: Enabled
Administrative Mode: private-vlan trunk promiscuous
Operational Mode: down
Administrative Trunking Encapsulation: negotiate
Negotiation of Trunking: on
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan secondary mapping: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: 1, 4, 3000-4000
Administrative private-vlan trunk private VLAN mappings:
    2 (VLAN0002)  3 (VLAN0003)          4 (VLAN0004)  5 (VLAN0005)
    10 (VLAN0010) 20 (CLAN0020)          30 (VLAN0030) 40 (Inactive)
Operational private-vlan: none

```

Related Commands

Command	Description
switchport mode	Sets the specified interfaces as either Layer 2 access or trunk interfaces.

show interface transceiver

To display information about all the transceiver interfaces, use the **show interface transceiver** command.

show interface transceiver [{**calibrations** | **details**}]

Syntax Description	
calibrations	(Optional) Displays calibration information for transceivers .
detail	(Optional) Displays detailed information for transceivers.

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	4.1(2)	This command was introduced.

Usage Guidelines This command does not require a license.

Examples This example shows how to display calibration information for transceiver interfaces:

```
switch(config)# show interface transceiver calibrations
Ethernet9/25
  sfp is present
  name is CISCO-EXCELIGHT
  part number is SPP5101LR-C1
  revision is A
  serial number is ECL121601PB
  nominal bitrate is 10300 Mbits/sec
  Link length supported for 9/125um fiber is 10 km(s)
  cisco id is --
  cisco extended id number is 4
  SFP External Calibrations Information
  -----
             Slope  Offset      Rx4/Rx3/Rx2/Rx1/Rx0
  -----
  Temperature      0      0
  Voltage           0      0
  Current           0      0
  Tx Power         0      0
  Rx Power                               0.0000/0.0000/0.0000/0.0000/0.0000
```

This example shows how to display detailed information for transceiver interfaces:

```
switch(config)# show interface transceiver detailed
Ethernet10/9
  sfp is present
  name is CISCO
  part number is SPP5101SR-C1
  revision is A
  serial number is ECL1120017J
  nominal bitrate is 10300 Mbits/sec
  Link length supported for 50/125um fiber is 82 m(s)
```

show interface transceiver

```

Link length supported for 62.5/125um fiber is 26 m(s)
cisco id is --
cisco extended id number is 4
      SFP Detail Diagnostics Information (external calibration)
-----
                Alarms                Warnings
                High                   Low                   High                   Low
-----
Temperature    25.54 C                75.00 C                -5.00 C                70.00 C                0.00 C
Voltage        3.22 V                  3.63 V                  2.97 V                  3.46 V                  3.13 V
Current        4.49 mA                   10.00 mA                 0.00 mA                 9.00 mA                 0.00 mA
Tx Power       -3.50 dBm                       2.99 dBm                -11.30 dBm              -1.00 dBm              -7.30 dBm
Rx Power       -2.92 dBm                       2.99 dBm                -13.97 dBm              -1.00 dBm              -9.91 dBm
Transmit Fault Count = 0
-----

```

Related Commands

Command	Description
show interface	Displays information about the specified interfaces.

show interface trunk

To display information about all the trunk interfaces, use the **show interface trunk** command.

show interface [**{ethernet***slot/port* | **port-channel***channel-number*}]**trunk**[**{module***number* | **vlan***vlan-id*}]

Syntax Description	Parameter	Description
	ethernet <i>slot/port</i>	(Optional) Type and number of the interface that you want to display .
	port-channel <i>channel-number</i>	(Optional) Specifies the port-channel number of the port-channel interface that you want to display.
	module <i>number</i>	(Optional) Specifies the module number. The range is from 1 to 18.
	vlan <i>vlan-id</i>	(Optional) Specifies the VLAN number. The range is from 1 to 2499 and from 2628 to 4093.

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	4.0	This command was introduced.

Usage Guidelines If you do not specify an interface, a module number, or a VLAN number, the system displays information for all trunk interfaces.

This command displays information about all Layer 2 trunk interfaces and trunk port-channel interfaces.

Use the **show interface counters** command to display statistics for the specified Layer 2 interface.

This command does not require a license.

Examples

This example shows how to display information for all Layer 2 trunk interfaces:

```
switch(config)# show interface trunk
-----
Port          Native  Status      Port
              Vlan                    Channel
-----
Eth2/9        1       trunking    --
Eth2/10       1       trnk-bndl   Po50
Po50          1       not-trunking --
-----
Port          Vlans Allowed on Trunk
-----
Eth2/9        1-3967,4048-4093
Eth2/10       1-3967,4048-4093
Po50          1-3967,4048-4093
-----
Port          STP Forwarding
-----
Eth2/9        none
```

show interface trunk

```
Eth2/10    none
Po50      none
```

Related Commands

Command	Description
switchport mode trunk	Sets the specified interfaces as Layer 2 trunk interfaces.

show interface tunnel

To display information about the tunnel interfaces, use the **show interface tunnel** command.

show interface tunnel *number*

Syntax Description	<i>number</i>	Number of the tunnel interface that you want to display information for. The range is from 0 to 65503.
---------------------------	---------------	--

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	4.2(1)	Display of configured static MAC address was added.
	4.1(2)	This command was introduced.

Usage Guidelines This command does not require a license.

Examples This example shows how to display information about tunnel interfaces:

```
switch(config)# show interface tunnel 5
Tunnel5 is down (Administratively down)
  MTU 1476 bytes, BW 9 Kbit
  Transport protocol is in VRF "default"
  Tunnel protocol/transport GRE/IP
  Last clearing of "show interface" counters never
  Tx
  0 packets output, 1 minute output rate 0 packets/sec
  Rx
  0 packets input, 1 minute input rate 0 packets/sec
```

Related Commands	Command	Description
	show interface	Displays information about the specified interfaces.

show ip dhcp snooping statistics

To display statistics related to the Dynamic Host Configuration Protocol (DHCP), use the **show ip dhcp snooping statistics** command.

show ip dhcp snooping statistics

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes EXEC mode

Command History	Release	Modification
	5.1(1)	Added the command output (added two counters)
	4.0	This command was introduced.

Usage Guidelines To enable this feature, use the **feature dhcp** command.

Examples This example shows how to display statistics related to DHCP:

```
switch# show ip dhcp snooping statistics
Packets processed 0
Packets received through cfsoe 0
Packets forwarded 0
Packets forwarded on cfsoe 0
Total packets dropped 0
Packets dropped from untrusted ports 0
Packets dropped due to MAC address check failure 0
Packets dropped due to Option 82 insertion failure 0
Packets dropped due to o/p intf unknown 0
Packets dropped which were unknown 0
Packets dropped due to dhcp relay not enabled 0
Packets dropped due to no binding entry 0
Packets dropped due to interface error/no interface 0
Packets dropped due to max hops exceeded 0
switch#
```

Related Commands	Command	Description
	show ip dhcp snooping statistics	Display statistics related to the Dynamic Host Configuration Protocol.

show lacp counters

To display information about Link Aggregation Control Protocol (LACP) statistics, use the **show lacp counters** command.

show lacp counters [**interface port-channel** *channel-number*]

Syntax Description	Parameter	Description
	interface port-channel	(Optional) Specifies the interface port channel.
	<i>channel-number</i>	(Optional) Number of the LACP channel group. The range is from 1 to 4096.

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	4.0	This command was introduced.

Usage Guidelines If you do not specify the *channel-number*, all channel groups are displayed.
This command does not require a license.

Examples

This example shows how to display the LACP statistics for a specific channel group:

```
switch# show lacp counters interface port-channel 1
LACPDUs      Marker      Marker Response  LACPDUs
Port         Sent       Recv      Sent   Recv    Sent   Recv    Pkts Err
-----
port-channell
Ethernet1/1   554       536        0      0       0       0       0
Ethernet1/2   527       514        0      0       0       0       0
Ethernet1/3   535       520        0      0       0       0       0
Ethernet1/4   515       502        0      0       0       0       0
Ethernet1/5   518       505        0      0       0       0       0
Ethernet1/6   540       529        0      0       0       0       0
Ethernet1/7   541       530        0      0       0       0       0
Ethernet1/8   547       532        0      0       0       0       0
Ethernet1/9   544       532        0      0       0       0       0
Ethernet1/10  513       501        0      0       0       0       0
Ethernet1/11  497       485        0      0       0       0       0
Ethernet1/12  493       486        0      0       0       0       0
Ethernet1/13  492       485        0      0       0       0       0
Ethernet1/14  482       481        0      0       0       0       0
Ethernet1/15  481       476        0      0       0       0       0
Ethernet1/16  482       477        0      0       0       0       0
```

Related Commands	Command	Description
	clear lacp counters	Clears the statistics for all LACP interfaces or those interfaces that belong to a specific LACP channel group.

show lacp interface

To display information about specific Link Aggregation Control Protocol (LACP) interfaces, use the **show lacp interface** command.

show lacpinterface ethernet slot/port

Syntax Description

<i>slot/port</i>	Slot number and port number for the interface you want to display. The range is from 1 to 253.
------------------	--

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

The LACP_Activity field displays whether the link is configured in the active or passive port-channel mode.

The Port Identifier field displays the port priority as part of the information. The part of the information in this field is the port number. The following example shows how to identify the port priority and the port number:

Port Identifier=0x8000,0x101

The port priority value is 0x8000, and the port number value is 0x101 in this example.

This command does not require a license.

Examples

This example shows how to display the LACP statistics for a specific channel group:

```
switch# show lacp interface ethernet 1/1
switch(config-if-range)# show lacp interface eth1/1
Interface Ethernet1/1 is up
  Channel group is 1 port channel is Po1
  PDUs sent: 556
  PDUs rcvd: 538
  Markers sent: 0
  Markers rcvd: 0
  Marker response sent: 0
  Marker response rcvd: 0
  Unknown packets rcvd: 0
  Illegal packets rcvd: 0
Lag Id: [ [(8000, 0-11-11-22-22-74, 0, 8000, 101), (8000, 0-11-11-22-22-75, 0, 8000, 401)] ]
Operational as aggregated link since Wed Jun 11 20:37:59 2008
Local Port: Eth1/1  MAC Address= 0-11-11-22-22-74
  System Identifier=0x8000,0-11-11-22-22-74
  Port Identifier=0x8000,0x101
  Operational key=0
  LACP_Activity=active
  LACP_Timeout=Long Timeout (30s)
  Synchronization=IN_SYNC
  Collecting=true
```

```
Distributing=true
Partner information refresh timeout=Long Timeout (90s)
Actor Admin State=
Actor Oper State=
Neighbor: 4/1
MAC Address= 0-11-11-22-22-75
System Identifier=0x8000,0-11-11-22-22-75
Port Identifier=0x8000,0x401
Operational key=0
LACP_Activity=active
LACP_Timeout=Long Timeout (30s)
Synchronization=IN_SYNC
Collecting=true
Distributing=true
Partner Admin State=
Partner Oper State=
```

Related Commands

Command	Description
show port-channel summary	Displays information about all port-channel groups.

show lacp neighbor

To display information about Link Aggregation Control Protocol (LACP) neighbors, use the **show lacp neighbor** command.

show lacp neighbor [**interface port-channel** *channel-number*]

Syntax Description	Parameter	Description
	interface port-channel	(Optional) Specifies the interface port channel.
	<i>channel-number</i>	(Optional) Port-channel number for the LACP neighbor that you want to display. The range is from 1 to 4096.

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	4.0	This command was introduced.

Usage Guidelines If you do not specify the *channel-number*, all channel groups are displayed. This command does not require a license.

Examples This example shows how to display the information about the LACP neighbors for a specific port channel:

```
switch# show lacp neighbor interface port-channel 1
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
port-channell neighbors
Partner's information
  Partner          Partner          Partner
Port System ID    Port Number    Age    Flags
Eth1/1 32768,0-11-11-22-22-750x401 44817 SA
      LACP Partner    Partner
      Port Priority    Oper Key    Port State
      32768            0x0        0x3d
Partner's information
  Partner          Partner          Partner
Port System ID    Port Number    Age    Flags
Eth1/2 32768,0-11-11-22-22-750x402 44817 SA
      LACP Partner    Partner
      Port Priority    Oper Key    Port State
      32768            0x0        0x3d
```

Related Commands	Command	Description
	show port-channel summary	Displays information about all port-channel groups.

show lacp port-channel

To display information about Link Aggregation Control Protocol (LACP) port channels, use the **show lacp port-channel** command.

show lacp port-channel [**interface port-channel** *channel-number*]

Syntax Description	interface port-channel	(Optional) Specifies the interface port channel.
	<i>channel-number</i>	(Optional) Port-channel number for the LACP neighbor that you want to display. The range is from 1 to 4096.

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	4.0	This command was introduced.

Usage Guidelines If you do not specify the *channel-number*, all channel groups are displayed. This command does not require a license.

Examples This example shows how to display the information about LACP port channels:

```
switch# show lacp port-channel
port-channel1
  Local System Identifier=0x8000,0-11-11-22-22-74
  Admin key=0x0
  Operational key=0x0
  Partner System Identifier=0x8000,0-11-11-22-22-75
  Operational key=0x0
  Max delay=0
  Aggregate or individual=1
port-channel2
  Local System Identifier=0x8000,0-11-11-22-22-74
  Admin key=0x1
  Operational key=0x1
  Partner System Identifier=0x8000,0-11-11-22-22-75
  Operational key=0x1
  Max delay=0
  Aggregate or individual=1
```

Related Commands	Command	Description
	show port-channel summary	Displays information about all port-channel groups.

show lacp summary

To display Link Aggregation Control Protocol (LACP) summary information, use the **show lacp summary** command.

show lacp [phy-port-vpc] summary

Syntax Description	phy-port-vpc (Optional) Displays information about the LACP status for the physical port VPC.
---------------------------	--

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	7.1(1)D1(0)	This command was introduced.

Usage Guidelines If the Link Aggregation Control Protocol (LACP) is not enabled, the output shows “NONE” in the Protocol column of the display.

A channel-group interface can be in the following operational states:

- Down—The interface is down because it is administratively shut down or some other reason not related to port channels.
- Individual—The interface is part of a port channel but is unable to aggregate into a port channel because of protocol exchange problems.
- Suspended—The operational parameters of the interface are not compatible with the port channel. This interface is not forwarding traffic, although the physical MAC link state is still up.
- Switched—The interface is switched.
- Up (port channel)—The port channel is up.
- Up in port channel (members)—The port member of the port channel is up.
- Hot standby (LACP only)—The interface is eligible to join the port group if one of the interfaces currently participating in the LACP channel goes down.
- Module-removed—The module has been removed.
- Routed—The interface is routed.

This command does not require a license.

Examples

This example shows how to display information about the LACP status for the physical port VPC :

```
switch(config)# show lacp phy-port-vpc summary
Flags:  D - Down          P - up
        s - Suspended    H - Hot-standby (LACP only)
        r - Module-removed
```


VPC-Id	Member Port
1	Eth1/1 (P)
2	Eth1/2 (H)
3	Eth1/3 (s)
4	Eth2/1 (r)

Related Commands

Command	Description
show lacp counters	Displays information about LACP statistics

show lacp system-identifier

To display the Link Aggregation Control Protocol (LACP) system identifier for the device, use the **show lacp system-identifier** command.

show lacp system-identifier

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Any command mode

Release	Modification
4.0	This command was introduced.

Usage Guidelines The LACP system ID is the combination of the configurable LACP system priority value and the MAC address.

Each system that runs LACP has an LACP system priority value. You can accept the default value of 32768 for this parameter, or you can configure a value between 1 and 65535. LACP uses the system priority with the MAC address to form the system ID and also uses the system priority during negotiation with other devices. A higher system priority value means a lower priority.

The system ID is different for each virtual device context (VDC).

This command does not require a license.

Examples

This example shows how to display the information about the LACP port channel for a specific port channel:

```
switch# show lacp system-identifier
8000,AC-12-34-56-78-90
```

Command	Description
lacp system-priority	Sets the system priority for LACP.

show ospfv3

To display general information about the Open Shortest Path First version 3 (OSPFv3) routing process, use the **show ospfv3** command.

```
show ospfv3 [process-id]
```

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Interface configuration mode

Command History	Release	Modification
	6.2(2)	This command was introduced.

Usage Guidelines OSPFv3 must be running on all participating devices. You must configure the he baseline parameters for Bidirectional Forwarding Detection (BFD) sessions on the interfaces over which you want to run BFD sessions to BFD neighbors must be configured.

Examples

This example shows how to display the general information about to discover the OSPFv3 routing process:

```
switch# configure terminal

switch(config)# interface ethernet 3/1
switch(config-router)# ospfv3 bfd disable
switch(config-if)# exit
switch(config)# show bfd neighbors details
switch(config)# show ospfv3
Routing Process 3 with ID 172.1.2.1 VRF default
Routing Process Instance Number 1
Stateful High Availability enabled
Graceful-restart is configured
Grace period: 60 state: Inactive
Last graceful restart exit status: None
Supports only single TOS(TOS0) routes
Supports opaque LSA
Administrative distance 110
Reference Bandwidth is 40000 Mbps
SPF throttling delay time of 200.000 msecs,
SPF throttling hold time of 1000.000 msecs,
SPF throttling maximum wait time of 5000.000 msecs
LSA throttling start time of 0.000 msecs,
LSA throttling hold interval of 5000.000 msecs,
LSA throttling maximum wait time of 5000.000 msecs
Minimum LSA arrival 1000.000 msec
LSA group pacing timer 10 secs
Maximum paths to destination 8
Number of external LSAs 0, checksum sum 0
Number of areas is 0, 0 normal, 0 stub, 0 nssa
Number of active areas is 0, 0 normal, 0 stub, 0 nssa
Install discard route for summarized external routes.
```

```

Install discard route for summarized internal routes.
BFD is enabled
Routing Process 200 with ID 172.1.2.1 VRF default
Routing Process Instance Number 2
Stateful High Availability enabled
Graceful-restart is configured
Grace period: 60 state: Inactive
Last graceful restart exit status: None
Supports only single TOS(TOS0) routes
Supports opaque LSA
Administrative distance 110
Reference Bandwidth is 40000 Mbps
SPF throttling delay time of 200.000 msec,
SPF throttling hold time of 1000.000 msec,
SPF throttling maximum wait time of 5000.000 msec
LSA throttling start time of 0.000 msec,
LSA throttling hold interval of 5000.000 msec,
LSA throttling maximum wait time of 5000.000 msec
Minimum LSA arrival 1000.000 msec
LSA group pacing timer 10 secs
Maximum paths to destination 8
Number of external LSAs 0, checksum sum 0
Number of areas is 0, 0 normal, 0 stub, 0 nssa
Number of active areas is 0, 0 normal, 0 stub, 0 nssa
Install discard route for summarized external routes.
Install discard route for summarized internal routes.
switch(config)#

```

Related Commands

Command	Description
ospfv3 bfd	Enables BFD on a per-interface basis for one or more interfaces associated with the OSPFv3 routing process.

show port-channel compatibility-parameters

To display the parameters that must be the same among the member ports in order to join a port channel, use the **show port-channel compatibility-parameters** command.

show port-channel compatibility-parameters

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	4.0	This command was introduced.

Usage Guidelines When you add an interface to a channel group, the software checks certain interface attributes to ensure that the interface is compatible with the channel group. For example, you cannot add a Layer 3 interface to a Layer 2 channel group. The software also checks the operational attributes for an interface before allowing that interface to participate in the port-channel aggregation.

This command displays the list of compatibility checks that the system uses.

Using the **channel-group** command, you can force ports with incompatible parameters to join the port channel as long as the following parameters are the same:

- (Link) speed capability
- Speed configuration
- Duplex capability
- Duplex configuration
- Flow-control capability
- Flow-control configuration



Note See the **channel-group** command for information about forcing ports to join a port channel.

This command does not require a license.

Examples

This example shows how to display the list of compatibility checks that the system makes to ensure that an interface is compatible with a channel group:

```
switch# show port-channel compatibility-parameters
* port mode
Members must have the same port mode configured, either E or AUTO. If they
are configured in AUTO port mode, they have to negotiate E mode when they
```

show port-channel compatibility-parameters

come up. If a member negotiates a different mode, it will be suspended.

- * speed

Members must have the same speed configured. If they are configured in AUTO speed, they have to negotiate the same speed when they come up. If a member negotiates a different speed, it will be suspended.

- * MTU

Members have to have the same MTU configured. This only applies to ethernet port-channel.

- * MEDIUM

Members have to have the same medium type configured. This only applies to ethernet port-channel.

- * Span mode

Members must have the same span mode.

- * sub interfaces

Members must not have sub-interfaces.

- * Duplex Mode

Members must have same Duplex Mode configured.

- * Ethernet Layer

Members must have same Ethernet Layer (switchport/no-switchport) configured.

- * Span Port

Members cannot be SPAN ports.

- * Storm Control

Members must have same storm-control configured.

- * Flow Control

Members must have same flowctrl configured.

- * Capabilities

Members must have common capabilities.

- * port

Members port VLAN info.

- * port

Members port does not exist.

- * switching port

Members must be switching port, Layer 2.

- * port access VLAN

Members must have the same port access VLAN.

- * port native VLAN

Members must have the same port native VLAN.

- * port allowed VLAN list

Members must have the same port allowed VLAN list.

Related Commands

Command	Description
channel-group	Adds or removes interfaces to port-channel groups and assigns the port-channel mode to the interface.

show port-channel database

To display information about the port channels, use the **show port-channel database** command.

show port-channel database [**interface port-channel** *channel-number*]

Syntax Description	interface port-channel	(Optional) Specifies the interface port channel.
	<i>channel-number</i>	(Optional) Port-channel number for the Link Aggregation Control Protocol (LACP) neighbor that you want to display. The range is from 1 to 4096.

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	4.0	This command was introduced.

Usage Guidelines If you do not specify the *channel-number*, all channel groups are displayed. This command displays Link Aggregation Control Protocol (LACP)-enabled ports channels and port channels without an associated aggregation protocol.

This command does not require a license.

Examples

This example shows how to display information about all port channels:

```
switch# show port-channel database
port-channel5
  Administrative channel mode is active
  Operational channel mode is active
  Last membership update is successful
  1 ports in total, 0 ports up
  Age of the port-channel is 1d:16h:18m:50s
  Time since last bundle is 1d:16h:18m:56s
  Last bundled member is
  Ports:  Ethernet2/5                [down]
port-channel20
  Administrative channel mode is active
  Operational channel mode is active
  Last membership update is successful
  1 ports in total, 0 ports up
  Age of the port-channel is 1d:16h:18m:50s
  Time since last bundle is 1d:16h:18m:56s
  Last bundled member is
  Ports:  Ethernet2/20              [down]
```

This example shows how to display information about a specific port channel:

```
switch# show port-channel database interface port-channel 20
port-channel20
  Administrative channel mode is active
```

```
Operational channel mode is active
Last membership update is successful
1 ports in total, 0 ports up
Age of the port-channel is 1d:16h:23m:14s
Time since last bundle is 1d:16h:23m:20s
Last bundled member is
Ports:  Ethernet2/20          [down]
```

Related Commands

Command	Description
show port-channel summary	Displays a summary of information about all port channels.

show port-channel load-balance

To display information about load balancing using port channels, use the **show port-channel load-balance** command.

show port-channel load-balance [**forwarding-path interface port-channel** *channel-number*]

Syntax Description	forwarding-path interface port-channel	(Optional) Identifies the port in the port channel that forwards the packet.
	<i>channel-number</i>	Port-channel number for the load-balancing forwarding path that you want to display. The is from 1 to 4096.

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	4.0	This command was introduced.

Usage Guidelines This command does not require a license.

Examples This example shows how to display information about the current port-channel load balancing for the system:

```
switch# show port-channel load-balance
Port Channel Load-Balancing Configuration:
System: source-dest-ip-vlan
Port Channel Load-Balancing Addresses Used Per-Protocol:
Non-IP: source-dest-mac
IP: source-dest-ip-vlan
```

Related Commands	Command	Description
	port-channel load-balance ethernet	Configures load balancing using port channels.

show port-channel rbh-distribution

To display information about the Result Bundle Hash (RBH) for port channels, use the **show port-channel rbh-distribution** command.

show port-channel rbh-distribution [**interface port-channel** *channel-number*]

Syntax Description	Parameter	Description
	interface port-channel	(Optional) Specifies the interface port channel.
	<i>channel-number</i>	(Optional) Port-channel number for the LACP neighbor that you want to display. The range is from 1 to 4096.

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	4.0	This command was introduced.

Usage Guidelines The RBH value ranges from 0 to 7 and is shared among port members in a port channel. This command does not require a license.

Examples This example shows how to display RBH distribution for a specific port channel:

```
switch# show port-channel rbh-distribution interface port-channel 4
ChanId   Member port   RBH values   Num of buckets
-----
4        Eth3/13      4,5,6,7     4
4        Eth3/14      0,1,2,3     4
```

Related Commands	Command	Description
	port-channel summary	Displays summary information about port channels.

show port-channel summary

To display summary information about the port channels, use the **show port-channel summary** command.

show port-channel summary

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	5.1(1)	Added a new port channel status 'M' to the command output.
	4.0	This command was introduced.

Usage Guidelines If the Link Aggregation Control Protocol (LACP) is not enabled, the output shows “**NONE**” in the Protocol column of the display.

A channel-group interface can be in the following operational states:

- Down—The interface is down because it is administratively shut down or some other reason not related to port channels.
- Individual—The interface is part of a port channel but is unable to aggregate into a port channel because of protocol exchange problems:
 - This interface continues to forward traffic as an individual link.
 - STP is aware of this interface.
- Suspended—The operational parameters of the interface are not compatible with the port channel. This interface is not forwarding traffic, although the physical MAC link state is still up.
- Switched—The interface is switched.
- Up (port channel)—The port channel is up.
- Up in port channel (members)—The port member of the port channel is up.
- Hot standby (LACP only)—The interface is eligible to join the port group if one of the interfaces currently participating in the LACP channel goes down.
 - This interface does not forward data traffic; it forwards only protocol data units (PDUs).
 - This interface does not run STP.
- Module-removed—The module has been removed.
- Routed—The interface is routed.

This command does not require a license.

Examples

This example shows how to display summary information for the port channels:

```
switch(config-if)# show port-channel summary
Flags: D - Down          P - Up in port-channel (members)
      I - Individual    H - Hot-standby (LACP only)
      s - Suspended     r - Module-removed
      S - Switched      R - Routed
      U - Up (port-channel)
      M - Not in use. Min-links not met
-----
```

Group Channel	Port-Channel	Type	Protocol	Member Ports
2	Po2 (SU)	Edge	LACP	Eth4/9 (D) Eth4/10 (D) Eth4/11 (P) Eth4/12 (P)
3	Po3 (SU)	Edge	LACP	Eth4/27 (P) Eth4/28 (P) Eth4/29 (P) Eth4/30 (P)
10	Po10 (SU)	Edge	LACP	Eth4/1 (P) Eth4/2 (P) Eth4/3 (P) Eth4/4 (P) Eth4/13 (P) Eth4/14 (P) Eth4/15 (P) Eth4/16 (P) Eth4/17 (P) Eth4/18 (P) Eth4/19 (P) Eth4/20 (P) Eth4/21 (P) Eth4/22 (P) Eth4/23 (P) Eth4/24 (P)

Related Commands

Command	Description
show port-channel usage	Displays the port-channel numbers used and available.
show port-channel traffic	Displays transmitted and received unicast, multicast, and broadcast percentages for the port channels.

show port-channel traffic

To display traffic statistics for port channels, use the **show port-channel traffic** command.

show port-channel traffic [**interface port-channel** *channel-number*]

Syntax Description	interface port-channel	(Optional) Specifies the interface port channel.
	<i>channel-number</i>	(Optional) Port-channel number for the LACP neighbor that you want to display. The range is from 1 to 4096.

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	4.0	This command was introduced.

Usage Guidelines This command displays the percentage of transmitted and received unicast, multicast, and broadcast traffic about the port channel.

If you do not specify the *channel-number*, information for all port channels is displayed.

This command does not require a license.

Examples

This example shows how to display the traffic statistics for all port channels:

```
switch(config)# show port-channel traffic
ChanId      Port  Rx-Ucst Tx-Ucst Rx-Mcst Tx-Mcst Rx-Bcst Tx-Bcst
-----
      5   Eth2/5   0.0%   0.0%   0.0%   0.0%   0.0%   0.0%
-----
     20  Eth2/20   0.0%   0.0%   0.0%   0.0%   0.0%   0.0%
```

This example shows how to display the traffic statistics for a specific port channel:

```
switch(config)# show port-channel traffic interface port-channel 5
ChanId      Port  Rx-Ucst Tx-Ucst Rx-Mcst Tx-Mcst Rx-Bcst Tx-Bcst
-----
      5   Eth2/5   0.0%   0.0%   0.0%   0.0%   0.0%   0.0%
```

Related Commands	Command	Description
	port-channel summary	Displays summary information about port channels.

show port-channel usage

To display the port-channel numbers used and available, use the **show port-channel usage** command.

show port-channel usage

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	4.0	This command was introduced.

Usage Guidelines This command displays port-channel numbers used and available in the virtual device context (VDC) that you are monitoring.

The number of port-channel numbers available across all VDCs for the entire system is from 1 to 4096.

This command does not require a license.

Examples

This example shows how to display the usage for all port channels:

```
switch# show port-channel usage
Totally 2 port-channel numbers used
=====
Used   :   5 , 20
Unused:   1 - 4 , 6 - 19 , 21 - 4096
```

Related Commands

Command	Description
port-channel summary	Displays summary information about port channels.

show port-profile

To display information about port profiles, use the **show port-profile** command.

show port-profile [{**brief** | **expand-interface** [**name name**] | **name name** | **usage**}]

Syntax Description	Parameter	Description
	brief	(Optional) Displays brief information about the port profiles.
	expand-interface name	(Optional) Displays the configured attributes at an interface per port profile. An optional name can be specified to show the expanded interface output for that specific port profile.
	name name	(Optional) Displays information for the specified port profile.
	usage	(Optional) Displays a list of interfaces to which each profile is attached.

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	4.2(1)	This command was introduced.

Usage Guidelines Use the **show port-profile** command to display information about the configured port profiles on the device. It displays all configured port profiles.

Port profiles are not aware of default values, so the default value configuration appears in the port profiles. For example, MTU 1500 is a default value and does not appear in the running-configuration of an interface. However, because port profiles are unaware of default values, MTU 1500 appears in the port-profile display.

This command does not require a license.

Examples

This example shows how to display information about port profiles:

```
switch(config)# show port-profile
try1
type: Ethernet
description:
status: enabled
max-ports: 512
inherit:
config attributes:
  channel-group 5
evaluated config attributes:
  channel-group 5
assigned interfaces:
  Ethernet1/1
try2
type: Ethernet
description:
status: disabled
max-ports: 512
```

```

inherit:
config attributes:
evaluated config attributes:
assigned interfaces:

```

This example shows how to display brief port profile information:

```

switch(config)# show port-profile brief
-----
Port          Profile  Conf   Eval   Assigned  Child
Profile       State   Items Items   Intfs     Profs
-----
try1          1       1      1      1         0
try2          0       0      0      0         0

```

This example shows how to display expanded port profile interface information:

```

switch(config)# show port-profile expand-interface
try1
Ethernet1/1
  channel-group 5
try2

```

This example shows how to display specific port profile information:

```

switch(config)# show port-profile name try1
try1
type: Ethernet
description:
status: enabled
max-ports: 512
inherit:
config attributes:
  channel-group 5
evaluated config attributes:
  channel-group 5
assigned interfaces:
  Ethernet1/1
switch(config)# show port-profile usage
try1
Ethernet1/1

```

This example shows how to display port profiles and values that you have entered in interface configuration mode using the **show running-config** command:

```

switch(config)# show running-config interface ethernet 8/5
interface ethernet8/5
  inherit try1
  mtu 3000

```

Related Commands

Command	Description
port-profile	Configures, names, and allows you to enter port-profile configuration mode.
inherit port-profile	Assigns port profile to specified interfaces and allows one port profile to inherit configuration parameters from another port profile.

show running-config bfd

To display the running BFD configuration, use the **show running-config bfd** command.

show running-config bfd [all]

Syntax Description	all Displays the default configurations.
---------------------------	---

Command Default	None
------------------------	------

Command Modes	Any command mode
----------------------	------------------

Command History	Release	Modification
	4.0	This command was introduced.

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples

This example shows how to display all the running BFD configurations:

```
switch# show running-config bfd all
!Command: show running-config bfd
!Time: Tue Nov 22 06:15:17 2016
version 8.0(1)
feature bfd
bfd interval 555 min_rx 555 multiplier 5
bfd slow-timer 2000
no bfd echo-interface
bfd echo-rx-interval 50
bfd c-bit
```

Related Commands	Command	Description
	bfdc-bit	Configures the independent control plane setting in outgoing BFD packets.

show running-config interface

To display the running configuration for a specific interface, use the **show running-config interface** command.

```
show running-config interface [{all | {ethernet {slot/port} [all]} | expand-port-profile |
{loopback {number} [all]} | {mgmt0 [all]} | {port-channel {channel-number} [membership]} |
{tunnel {number} [all]} | {vlan {vlan-id} [all]}}]
```

Syntax Description

all	(Optional) Displays the configuration with defaults.
ethernet <i>slot/port</i>	Displays the number of the module and port number. The range is from 1 to 253.
expand-port-profile	(Optional) Displays port profiles.
loopback <i>number</i>	Displays the number of the loopback interface. The range is from 1 to 4096.
mgmt0	(Optional) Displays the management interface.
port-channel <i>channel-number</i>	Displays the number of the port-channel group. The range is from 0 to 1023.
membership	(Optional) Specifies the membership of the specified port channel.
tunnel <i>number</i>	Displays the number of the tunnel interface. The range is from 0 to 65535.
vlan <i>vlan-id</i>	Displays the number of the VLAN. The range is from 1 to 4096.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0	This command was introduced.
4.2(1)	The expand-port-profile parameter was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display information about the running configuration for a specific Ethernet interface:

```
switch(config)# show running-config interface ethernet 2/7
version 4.0(3)
interface Ethernet2/7
  description Ethernet port 3 on module 1
  mtu 8000
  delay 20
  udld enable
  no shutdown
```

This example shows how to display information about the running configuration for a specific range of Ethernet interfaces:

```
switch(config)# show running-config interface ethernet 2/7 - 9
version 4.0(3)
interface Ethernet2/7
  description Ethernet port 3 on module 1
  mtu 8000
  delay 20
  udd enable
  no shutdown
interface Ethernet2/8
  no shutdown
interface Ethernet2/9
  no shutdown
```

This example shows how to display information about the running configuration for a specific loopback interface:

```
switch(config)# interface loopback 345
switch(config-if)# show running-config interface loopback 345
version 4.0(3)
interface loopback345
```

This example shows how to display the running configuration for a specific port channel:

```
switch(config)#
show running-config interface port-channel 10
version 4.0(1)
interface port-channel10
  switchport
  switchport mode trunk
```

This example shows how to display information about the running configuration for VLAN interface 50:

```
switch(config)# show running-config interface vlan 50
version 4.0(3)
interface Vlan50
```

Related Commands

Command	Description
interface	Enters the interface configuration mode and configures the types and identities of interfaces.
interface vlan	Creates a VLAN interface and enters interface configuration mode.
show interface ethernet	Displays information about the Ethernet interface.
show port-channel summary	Displays a summary of port-channel information.
show running-config	Displays the running configuration on the device.

show running-config interface mgmt

To display the running configuration for a specific management interface, use the **show running-config interface mgmt** command.

showrunning-config *interfacemgmtnumber*

Syntax Description

<i>number</i>	Management interface number that you want to display. The value is from 0 to 0.
---------------	---

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **show running-config interface mgmt** command to display the running configuration for a management interface.

This command does not require a license.

Examples

This example shows how to display information about the running configuration for management interface 0:

```
switch# show running-config interface mgmt 0
version 4.0(3)
interface mgmt0
  ip address 172.28.231.193/23
```

Related Commands

Command	Description
show interface mgmt	Displays the management interface information.

show running-config vpc

To display the running configuration information for virtual port channels (vPCs), use the **show running-config vpc** command.

show running-config vpc [all]

Syntax Description	all (Optional) Displays the running configuration for all vPCs.
---------------------------	--

Command Default	None
------------------------	------

Command Modes	Any command mode.
----------------------	-------------------

Command History	Release	Modification
	4.1(3)	This command was introduced.

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples This example shows how to display the running configuration for a vPC:

```
switch (config)# show running-config vpc
version 4.1(2)
feature vpc
vpc domain 2
role priority 1
system-priority 32667
peer-keepalive destination 10.10.76.52 source 10.10.76.51 udp-port 3200 vrf ma
engagement interval 1000 timeout 5
interface port-channel10
vpc 20
interface port-channel101
vpc 101
interface port-channel200
vpc peer-link
interface port-channel201
vpc 201
```

Related Commands	Command	Description
	show vpc brief	Displays information about vPCs. If the feature is not enabled, this command returns an error.

show running-config vpc-config-sync

To display the virtual port channels (vPC) configuration synchronization-related configuration in the running configuration, use the **show running-config vpc-config-sync** command.

show running-config vpc-config-sync

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Any command mode.

Command History	Release	Modification
	7.1(1)D1(0)	This command was introduced.

Usage Guidelines This command does not require a license.

Examples This example shows how to display vPC configuration synchronization-related configuration in the running configuration:

```
switch# show running-config vpc-config-sync
!Time: Wed Jul 23 10:01:08 2014
version 7.1(0)D1(1)
vpc domain 10
  config-sync
```

Related Commands	Command	Description
	config-sync	Enables vPC configuration synchronization.

show startup-config interface

To display interface configuration information in the startup configuration, use the **show startup-config interface** command.

show startup-config interface [{ethernet *slot/port* | **expand-port-profile** | *loopback number* | **mgmt** | **port-channel** {*channel-number*} [**membership**] | *tunnel number* | {**vlan** *vlan-id*}]

Syntax Description		
ethernet <i>slot/port</i>	(Optional) Displays the number of the module and port number.	
expand-port-profile	(Optional) Displays the port profiles.	
loopback <i>number</i>	(Optional) Displays the number of the loopback interface. The range is from 1 to 4096.	
mgmt	(Optional) Displays the management interface.	
port-channel <i>channel-number</i>	(Optional) Displays the number of the port-channel group. The range is from 0 to 1023.	
membership	(Optional) Displays the membership of the specified port channel.	
tunnel <i>number</i>	(Optional) Displays the number of the tunnel interface. The range is from 0 to 65535.	
vlan <i>vlan-id</i>	(Optional) Displays the number of the VLAN. The range is from 1 to 4096.	

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	4.1(2)	This command was introduced.
	4.2(1)	The expand-port-profile parameter was introduced.

Usage Guidelines This command does not require a license.

Examples

This example shows how to display the information in the startup configuration for the interface Ethernet 7/1:

```
switch(config)# show startup-config interface ethernet 7/1
version 4.1(2)
interface Ethernet7/1
    ip pim sparse-mode
```

Related Commands

Command	Description
show interface	Displays information about the specified interface.

show startup-config vpc

To display virtual port-channel (vPC) configuration information in the startup configuration, use the **show startup-config vpc** command.

show startup-config vpc [all]

Syntax Description	all (Optional) Displays the startup-configuration information for all vPCs.
---------------------------	--

Command Default	None
------------------------	------

Command Modes	Any command mode
----------------------	------------------

Command History	Release	Modification
	4.1(3)	This command was introduced.

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples This example shows how to display the vPC information in the startup configuration:

```
switch(config)# show startup-config vpc
version 4.1(2)
feature vpc
vpc domain 1
interface port-channel10
    vpc peer-link
interface port-channel20
    vpc 100
```

Related Commands	Command	Description
	show vpc brief	Displays information about vPCs.

show udd

To display information about the Unidirectional Link Detection (UDLD) configuration, use the **show udd** command.

show udd [*{ethernet slot/port | global | neighbors}*]

Syntax Description

ethernet <i>slot/port</i>	(Optional) Displays the Ethernet slot and port number you want to display. The range is from 1 to 253.
global	(Optional) Displays the UDLD global status and configuration on all interfaces.
neighbors	(Optional) Displays the UDLD neighbor interfaces.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **show udd** command to display information about the UDLD configuration for an interface. UDLD must be enabled on the device before you can display this command; enter the **feature udd** command to enable UDLD globally on the device.

This command does not require a license.

Examples

This example shows how to display information about the UDLD configuration for Ethernet port 2/7:

```
switch# show udd ethernet 2/7
Interface Ethernet2/7
-----
Port enable administrative configuration setting: disabled
Port enable operational state: disabled
Current bidirectional state: unknown
Current operational state: udld-init - Multiple neighbor not detected
Message interval: 7
Timeout interval: 5
```

Related Commands

Command	Description
udd	Configures the ports to use a UDLD mode.
feature udd	Enables UDLD globally on device.

show vdc

To display virtual device contexts (VDCs), use the **show vdc** command.

show vdc

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	5.1(1)	This command was introduced.

Usage Guidelines This command does not require a license.

Examples This example shows how to display VDCs:

```
switch# show vdc
Switchwide mode is m1 f1 m1x1 f2 m2x1
vdc_id  vdc_name                state      mac
  type      lc
-----  -----
-----  -----
1      switch                    active     00:22:55:79:a4:c1
  Ethernet m1 f1 m1x1 m2x1
2      2                            active     00:22:55:79:a4:c2
  Ethernet m1 f1 m1x1 m2x1
switch#
```

Related Commands	Command	Description
	show lACP	Displays LACP information.

show vpc brief

To display brief information about the virtual port channels (vPCs), use the **show vpc brief** command.

show vpc brief [*vpc number*]

Syntax Description	vpc number	(Optional) Displays brief information about the specified vPC. The range is from 1 to 4096.
---------------------------	-------------------	---

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	6.1(2)E1	Added an example with the fabricpath load balance command and the no port-channel limit command.
	6.1(2)	Changed the command output.
	4.2(1)	Added the vpc keyword and <i>number</i> argument.
	4.1(3)	This command was introduced.

Usage Guidelines The **show vpc brief** command displays the vPC domain ID, the peer-link status, the keepalive message status, whether the configuration consistency is successful, and whether the peer-link formed or failed to form.

This command is not available if you have not enabled the vPC feature. See the **feature vpc** command for information on enabling vPCs.

Beginning with Cisco Release 4.2(1), you can display the track object, if you have configured a tracked object for running vPCs on a single module under the vpc-domain configuration mode.

This command does not require a license.

Examples

This example shows how to display brief information about the vPCs:

```
switch(config)# show vpc brief
switch-peer1(config)# show vpc brief
Legend:
      (*) - local vPC is down, forwarding via vPC peer-link
vPC domain id           : 1
vPC+ switch id         : 2
Peer status             : peer adjacency formed ok
vPC keep-alive status   : peer is alive
vPC fabricpath status   : peer is reachable through fabricpath
Configuration consistency status : success
Per-vlan consistency status : success
Type-2 inconsistency reason : Consistency Check Not Performed
vPC role                : primary
Number of vPCs configured : 8
Peer Gateway            : Disabled
Dual-active excluded VLANs : -
```

```
Graceful Consistency Check      : Enabled
Auto-recovery status           : Disabled
Fabricpath load balancing       : Enabled
Port Channel Limit             : limit to 244
vPC Peer-link status
```

```
-----
id  Port   Status Active vlans
--More-
```

This example shows how to displays brief information about the vPCs when the fabricpath load balance command and the no port-channel limit command are configured:

```
switch(config-vpc-domain)# show vpc
Legend:
(*) - local vPC is down, forwarding via vPC peer-link
vPC domain id : 1
vPC+ switch id : 1
Peer status : peer adjacency formed ok
vPC keep-alive status : peer is alive
vPC fabricpath status : peer is not reachable through fabricpath
Configuration consistency status : success
Per-vlan consistency status : success
Type-2 consistency status : success
vPC role : secondary
Number of vPCs configured : 1
Peer Gateway : Disabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
Auto-recovery status : Disabled
Fabricpath load balancing : Enabled
Operational Layer3 Peer : Disabled
Port Channel Limit : no limit
vPC Peer-link status
-----
id Port Status Active vlans
```

```
-----
1 Po100 up 1-10
vPC status
```

```
-----
id Port Status Consistency Reason Active vlans vPC+ Attribute
-----
1 Po1 up success success 1-10 DF: Partial, FP
MAC: 1.1.4513
```

This example shows how to display brief information about the vPCs when no port-channel limit is added:

```
switch-peer1(config-vpc-domain)# no port-channel limit
switch-peer1(config-vpc-domain)# show vpc brief
Legend:
(*) - local vPC is down, forwarding via vPC peer-link
vPC domain id      : 1
vPC+ switch id    : 2
Peer status        : peer adjacency formed ok
vPC keep-alive status : peer is alive
vPC fabricpath status : peer is reachable through fabricpath
Configuration consistency status : success
Per-vlan consistency status : success
Type-2 inconsistency reason : Consistency Check Not Performed
vPC role           : primary
```


Related Commands

Command	Description
feature vpc	Enables vPCs on the device.
show port channel summary	Displays information about port channels.

show vpc config-sync

To display information relating to the virtual port channels (vPC) configuration synchronization process, use the **show vpc config-sync** command.

show vpc config-sync {status | cli syntax | database | merge status}

Syntax Description	status	cli syntax	database	merge status
	Displays the status of the last 10 operations performed by the configuration synchronization process.	Displays the list of commands that are able to be configuration synchronized.	Displays the configuration synchronization database.	Displays the status of the merge with each peer switch.

Command Default None

Command Modes Any command mode.

Command History	Release	Modification
	7.1(1)D1(0)	This command was introduced.

Usage Guidelines This command does not require a license.

Examples This example shows how to display the list of commands that are able to be configuration synchronized:

```
(config)# show vpc config-sync cli syntax
MODE configuration terminal
(1) [ no ] spanning-tree mode [ <stp-mode> ]
(2) [ no ] spanning-tree { vlan <vlan-id> | bridge-domain <bd-id> } priority [ <prio> ]
(3) no spanning-tree mst configuration
(4) [ no ] spanning-tree { vlan <vlan-id> | bridge-domain <bd-id> }
(5) [ no ] spanning-tree port type edge default
(6) [ no ] spanning-tree port type edge bpduguard default
(7) [ no ] spanning-tree port type edge bpdufilter default
(8) [ no ] spanning-tree port type network default
(9) [ no ] spanning-tree bridge assurance
(10) [ no ] spanning-tree mst simulate pvst global
(11) [ no ] spanning-tree loopguard default
(12) spanning-tree mst configuration
(13) instance <instance-id> vlan <vlan-list>
(14) no instance <instance-id> [ vlan <vlan-list> ]
(15) [ no ] name [ <name-val> ]
(16) [ no ] revision [ <rev-id> ]
MODE interface ethernet
(17) no switchport
(18) [ no ] spanning-tree mst simulate pvst [ <simpvst-disable> ]
(19) [ no ] spanning-tree port type [ <port-type> ]
(20) [ no ] spanning-tree port type edge [ trunk ]
```



```

(21) [ no ] spanning-tree guard [ <guard-type> ]
(22) switchport
(23) [ no ] duplex [ <duplex_mode> ]
(24) [ no ] mtu [ <mtu_val> ]
(25) [ no ] speed [ { <speed_val> | auto [ 10 100 [ 1000 ] ] } ]
(26) [ no ] switchport vlan mapping enable
(27) [ no ] vpc <vpc_num>
(28) [ no ] switchport access vlan
(29) [ no ] switchport mode
(30) [ no ] switchport mode fex-fabric
MODE interface port-channel
(31) switchport
(32) no switchport
(33) [ no ] duplex [ <duplex_mode> ]
(34) [ no ] mtu [ <mtu_val> ]
(35) [ no ] speed [ { <speed_val> | auto [ 10 100 [ 1000 ] ] } ]
(36) [ no ] vpc [ <vpc_num> ]
(37) [ no ] switchport mode fex-fabric
(38) [ no ] switchport vlan mapping enable
(39) [ no ] vpc peer-link
(40) [ no ] switchport mode
(41) [ no ] switchport access vlan
(42) [ no ] spanning-tree mst simulate pvst [ <simpvst-disable> ]
(43) [ no ] spanning-tree port type [ <port-type> ]
(44) [ no ] spanning-tree port type edge [ trunk ]
(45) [ no ] spanning-tree guard [ <guard-type> ]
MODE vpc-domain
(46) [ no ] graceful consistency-check
(47) [ no ] peer-switch
(48) [ no ] system-mac
(49) [ no ] system-priority
(50) [ no ] dual-active exclude interface-vlan
(51) [ no ] peer-gateway
(52) [ no ] layer3 peer-router
(53) [ no ] self-isolation
(54) [ no ] delay restore
(55) [ no ] delay restore interface-vlan
(56) [ no ] mode auto
(57) [ no ] fabricpath switch-id [ <es_id> ]
(58) [ no ] fabricpath multicast load-balance
(59) [ no ] auto-recovery [ reload-delay <time-out> ]

```

This example shows how to display the configuration synchronization database:

```

switch(config)# show vpc config-sync database
Config-sync Database:
-----
Distribution: Enabled
Mode: Sync
Features synced:
  sync-feature vpc always-sync
  sync-feature vpc-type-1 always-sync
Interfaces synced:
  interface port-channel400
    vpc 400
  interface port-channel300
    vpc 300

```

This example shows how to display the status of the merge with each peer switch:

```

switch(config)# show vpc config-sync merge status
System merge status : Peer partially in-sync
Failure reason      : Conflicting configuration on peer switch.

```

```
Local switch config:
  interface port-channel300
    speed 10000
    mtu 9200
Peer switch config :
  interface port-channel300
    speed 1000
    mtu 9216
Global configuration : Peer in-sync
Interface merge status:
  interface port-channel400 : Peer in-sync
  interface port-channel300 : Peer out-of-sync
```

Related Commands

Command	Description
config-sync	Enables vPC configuration synchronization.

show vpc consistency-parameters

To display the consistency of parameters that must be compatible across the virtual port-channel (vPC) interfaces, use the **show vpc consistency-parameters** command.

```
show vpc consistency-parameters {global | interface port-channel channel-number | vlan | vpc
number}
```

Syntax Description	Parameter	Description
	global	(Optional) Displays the configuration of all Type 1 global parameters on both sides of the vPC peer link.
	interfaceport-channel	(Optional) Displays the configuration of all Type 1 interface parameters on both sides of the vPC peer link.
	<i>channel-number</i>	(Optional) Channel number. The range is from 1 to 4096.
	vlan	(Optional) Displays the configuration of all Type 1 interface parameters on both sides of the vPC peer link for the specified VLAN.
	vpc number	(Optional) Displays the configuration of all Type 1 interface parameters on both sides of the vPC peer link for the specified vPC. The range is from 1 to 4096.

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	4.1(3)	This command was introduced.
	4.2(1)	Added the display of local suspended VLANs. Note The command does not display the vPC peer device's suspended VLANs.
	4.2(1)	Added the <i>vpc</i> argument.
	5.2(1)	Added the vlan keyword.

Usage Guidelines The **show vpc consistency-parameters** command displays the configuration of all the vPC Type 1 parameters on both sides of the vPC peer link.



Note All the Type 1 configurations must be identical on both sides of the vPC peer link, or the link does not come up.

The vPC Type 1 configuration parameters are as follows:

- Port-channel mode: on, off, or active

- Link speed per channel
- Duplex mode per channel
- Trunk mode per channel
 - Native VLAN
 - VLANs allowed on trunk
 - Tagging of native VLAN traffic
- Spanning Tree Protocol (STP) mode
- STP region configuration for Multiple Spanning Tree
- Enable/disable state the same per VLAN
- STP global settings
 - Bridge Assurance setting
 - Port type setting—We recommend that you set all vPC peer link ports as network ports.
 - Loop Guard settings
- STP interface settings:
 - Port type setting
 - Loop Guard
 - Root Guard
- Maximum transmission unit (MTU)
- Allowed VLAN bit set

This command is not available if you have not enabled the vPC feature. See the **feature vpc** command for information on enabling vPCs.

This command does not require a license.

Examples

This example shows how to display the vPC consistency parameters for the specified port channel:

```
switch (config)# show vpc consistency-parameters global
Legend:
      Type 1 : vPC will be suspended in case of mismatch
Name      Type Local Value      Peer Value
-----
STP Mode   1      Rapid-PVST      Rapid-PVST
STP Disabled 1      None            None
STP MST    1      ""              ""
Region Name
STP MST    1      0              0
Region
Revision
STP MST    1
Region
Instance to
```

```

VLAN Mapping
STP Loopguard 1 Disabled Disabled
STP Bridge 1 Enabled Enabled
Assurance
STP Port Type 1 Normal Normal
Allowed VLAN - 1-100 1-100
Local suspended - 1-50 -
VLANs

```

This example shows how to display the vPC consistency parameters for the specified port channel:

```

switch (config)# show vpc consistency-parameters interface port-channel 20
Legend:

```

```

Type 1 : vPC will be suspended in case of mismatch
Name      Type Local Value      Peer Value
-----
STP Port Type 1 Default      Default
STP Port   1 None         None
Guard
mode       1 on          on
Speed     1 10 Gb/s    10 Gb/s
Duplex    1 full      full
Port Mode 1 trunk     trunk
Native Vlan 1 1         1
MTU       1 1500     1500
Allowed VLAN - 1-100    1-100
bitset

```

Related Commands

Command	Description
show vpc brief	Displays information about vPCs. If the feature is not enabled, the system displays an error when you enter this command.
show port channel summary	Displays information about port channels.

show vpc orphan-ports

To display ports that are not part of the virtual port channel (vPC) but have common VLANs, use the **show vpc orphan-ports** command.

show vpc orphan-ports

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	4.2(1)	This command was introduced.

Usage Guidelines The **show vpc orphan-ports** command displays those ports that are not part of the vPC but that share common VLANs with ports that are part of the vPC.

This command is not available if you have not enabled the vPC feature. See the **feature vpc** command for information on enabling vPCs.

This command does not require a license.

Examples

This example shows how to display vPC orphan ports:

```
switch(config)# show vpc orphan ports
Note:
-----::Going through port database. Please be patient.::-----
VLAN          Orphan Ports
-----
1             Po600
2             Po600
3             Po600
4             Po600
5             Po600
6             Po600
7             Po600
8             Po600
9             Po600
10            Po600
11            Po600
12            Po600
13            Po600
14            Po600
15            Po600
```

Related Commands	Command	Description
	feature vpc	Enables vPCs on the device.

Command	Description
show vpc brief	Displays brief information about vPCs.

show vpc peer-keepalive

To display the destination IP for the virtual port-channel (vPC) peer keepalive message and the status of the messages, use the **show vpc peer-keepalive** command.

show vpc peer-keepalive

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Any command mode

Release	Modification
4.1(3)	This command was introduced.

Usage Guidelines The show **vpc peer-keepalive** command displays the destination IP of the peer keepalive message for the vPC. The command also displays the send and receive status as well as the last update from the peer in seconds and milliseconds



Note We recommend that you create a separate virtual routing and forwarding (VRF) instance on the peer devices to send and receive the vPC peer keepalive messages. Do not use the peer link itself to send the vPC peer-keepalive messages.

This command is not available if you have not enabled the vPC feature. See the **feature vpc** command for information on enabling vPCs.

This command does not require a license.

Examples

This example shows how to display information about the peer-keepalive message:

```
n7k-2(config-vpc-domain)# show vpc peer-keepalive
vPC keep-alive status          : peer is alive
--Send status                  : Success
--Last send at                 : 2008.05.17 18:23:53 986 ms
--Sent on interface            : Eth7/16
--Receive status               : Success
--Last receive at              : 2008.05.17 18:23:54 99 ms
--Received on interface        : Eth7/16
--Last update from peer        : (0) seconds, (486) msec
vPC Keep-alive parameters
--Destination                   : 172.23.145.213
--Keepalive interval            : 1000 msec
--Keepalive timeout             : 5 seconds
--Keepalive hold timeout        : 3 seconds
--Keepalive vrf                 : pkal
--Keepalive udp port            : 3200
--Keepalive tos                 : 192
```


Related Commands

Command	Description
show vpc brief	Displays information about vPCs. If the feature is not enabled, the system displays an error when you enter this command.

show vpc role

To display information about the virtual port-channel (vPC) role of the peer device, use the **show vpc role** command.

show vpc role

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Any command mode

Release	Modification
4.1(3)	This command was introduced.

Usage Guidelines The **show vpc role** command displays the following information about the vPC status:

- Status of peer adjacency
- vPC role of the VDC that you are working on
- vPC MAC address
- vPC system priority
- MAC address of the device that you are working on
- System priority for the device that you are working on

This command is not available if you have not enabled the vPC feature. See the **feature vpc** command for information on enabling vPCs.

This command does not require a license.

Examples

This example shows how to display the vPC role information of the device that you are working on:

```
switch (config)# show vpc role

Primary:
vPC Role status
-----
vPC role                : primary
Dual Active Detection Status : 0
vPC system-mac          : 00:23:04:ee:be:01
vPC system-priority     : 32667
vPC local system-mac    : 00:22:55:79:ea:c1
vPC local role-priority : 32667
Secondary:
vPC Role status
-----
vPC role                : secondary
Dual Active Detection Status : 0
```

```
vPC system-mac           : 00:23:04:ee:be:01
vPC system-priority      : 32667
vPC local system-mac     : 00:22:55:79:de:41
vPC local role-priority  : 32667
```

When you reload the primary vPC peer device, the secondary vPC peer device assumes the role of the primary device. The following example shows how the vPC role displays on the new primary device:

```
switch (config)# show vpc role

vPC Role status
-----
vPC role           : secondary, operational primary
Dual Active Detection Status : 0
vPC system-mac     : 00:23:04:ee:be:64
vPC system-priority : 32667
vPC local system-mac : 00:22:55:79:de:41
vPC local role-priority : 32667
```

Related Commands

Command	Description
show vpc brief	Displays information about vPCs. If the feature is not enabled, the system displays an error when you enter this command.
show port channel summary	Displays information about port channels.

show vpc statistics

To display virtual port-channel (vPC) statistics, use the **show vpc statistics** command.

show vpc statistics {**peer-keepalive** | **peer-link** | **vpc number**}

Syntax Description

peer-keepalive	Displays statistics about the peer-keepalive message.
peer-link	Displays statistics about the peer link.
vpc number	Displays statistics about the specified vPC. The range is from 1 to 4096.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.1(3)	This command was introduced.

Usage Guidelines

The **peer-link** parameter displays the same information as the **show interface port-channel channel number** command for the vPC peer-link port channel.

The **vpc number** parameter displays the same information as the **show interface port-channel channel number** command for the specified vPC port channel.

This command is not available if you have not enabled the vPC feature. See the **feature vpc** command for information on enabling vPCs.

This command does not require a license.

Examples

This example shows how to display statistics about the peer-keepalive message:

```
switch# show vpc statistics peer-keepalive
vPC keep-alive status          : peer is alive
VPC keep-alive statistics
-----
peer-keepalive tx count:      1036
peer-keepalive rx count:      1028
average interval for peer rx:  995
Count of peer state changes:   1
```

Related Commands

Command	Description
show vpc brief	Displays information about vPCs. If the feature is not enabled, the system displays an error when you enter this command.
show port channel summary	Displays information about port channels.



T Commands

- [track](#), on page 326
- [tunnel destination](#), on page 328
- [tunnel mode](#), on page 329
- [tunnel path-mtu-discovery](#), on page 330
- [tunnel source](#), on page 332
- [tunnel ttl](#), on page 333
- [tunnel use-vrf](#), on page 334

track

To configure the system to monitor the track-list object that contains all the virtual port-channel (vPC) links to the core and to the vPC peer link when you are using only a single module for all links, use the **track** command. To return to the default, use the **no** form of this command.

track track-object-id
no track track-object-id

Syntax Description

<i>track-object-id</i>	Track-list object that you already configured.
------------------------	--

Command Default

No tracking

Command Modes

vpc configuration mode

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

Beginning with Release 4.2, if you must configure all the vPC peer links and core-facing interfaces on a single N7K-M132XP-12 module, you should configure a track object and a track list that is associated with the Layer 3 link to the core and on all vPC peer links on both vPC peer devices. You can use this configuration to avoid dropping traffic if that particular module goes down because when all the tracked objects on the track list go down, the system does the following:

- Stops the vPC primary peer device sending peer-keepalive messages, which forces the vPC secondary peer device to take over.
- Brings down all the downstream vPCs on that vPC peer device, which forces all the traffic to be rerouted in the access switch to the other vPC peer device.

Once you configure this feature and if the module fails, the system automatically suspends all the vPC links on the primary vPC peer device and stops the peer-keepalive messages. This action forces the vPC secondary device to take over the primary role and all the vPC traffic to go to this new vPC primary device until the system stabilizes.

Create a track list that contains all the links to the core and all the vPC peer links as its object. Enable tracking for the specified vPC domain for this track list. Apply this same configuration to the other PC peer device.

This command does not require a license.

Examples

This example shows how to put the previously configured track-list object into the vPC domain on the vPC peer device:

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# track object 5
```

Related Commands

Command	Description
show vpc brief	Displays information about a vPC tracked object.
feature vpc	Enables vPCs on the device.

tunnel destination

To configure the destination endpoint for a tunnel, use the **tunnel destination** command. To remove the tunnel destination, use the **no** form of this command.

tunnel destination {ip-address | host-name}
no tunnel destination {ip-address | host-name}

Syntax Description

<i>ip-address</i>	IP address for the tunnel destination.
<i>host-name</i>	Hostname for the tunnel destination.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **tunnel destination** command to configure the destination address for an IP tunnel.

You should not have two tunnels using the same encapsulation mode with the same source and destination address.

This command requires the Enterprise license.

Examples

This example shows how to configure the tunnel destination:

```
switch(config-if)# tunnel destination 192.0.2.120
```

Related Commands

Command	Description
tunnel source	Sets the source of the IP tunnel.
interface tunnel	Creates the IP tunnel.
show interface tunnel	Displays information about the traffic about the specified tunnel interface.

tunnel mode

To configure the tunnel encapsulation mode for a tunnel, use the **tunnel mode** command. To restore the default value, use the **no** form of this command.

```
tunnel mode gre {ip | ipv6}
no tunnel mode gre {ip | ipv6}
```

Syntax Description	ip	Configures this tunnel encapsulation mode as IPv4.
	ipv6	Configures this tunnel encapsulation mode as IPv6.

Command Default None

Command Modes Interface configuration mode

Command History	Release	Modification
	4.0	This command was introduced.

Usage Guidelines Use the **tunnel mode** command to configure the tunnel encapsulation mode for a tunnel. This command requires the Enterprise license.

Examples

This example shows how to configure the tunnel mode:

```
switch(config-if)# tunnel mode gre ip
```

Related Commands	Command	Description
	tunnel destination	Sets the destination of the IP tunnel.
	interface tunnel	Creates the IP tunnel.
	show interface tunnel	Displays information about the traffic about the specified tunnel interface.

tunnel path-mtu-discovery

To enable Path MTU Discovery (PMTUD) on a tunnel interface, use the **tunnel path-mtu-discovery** command. 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 [{age-timer {aging-mins | infinite} | min-mtu mtu-bytes}]

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.
<i>aging-mins</i>	Number of minutes. The range is from 10 to 30. The default is 10.
infinite	Disables the age timer.
min-mtu <i>mtu-bytes</i>	(Optional) Specifies the minimum Path MTU across GRE tunnels. The range is from 92 to 65535 bytes. The default is 92.

Command Default

Disabled

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

When PMTUD (RFC 1191) is enabled on a tunnel interface, the router performs PMTUD processing for the 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. PMTUD maximizes 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 that 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** keyword sets a low limit through the MTU that can be learned through the PMTUD process. Any ICMP signal received that specifies an MTU less than the minimum MTU configured is ignored. You can use this feature to prevent a denial-of-service attack from any node that can send an ICMP message to the router that specifies a very small MTU.



Note PMTUD on a tunnel interface requires that the tunnel endpoint is able to receive ICMP messages generated by routers in the path of the tunnel. You should check that ICMP messages can be received before you use PMTUD over firewall connections.

This command requires the Enterprise license.

Examples

This example shows how to configure PMTUD:

```
switch(config-if)# tunnel path-mtu-discovery
```

Related Commands

Command	Description
tunnel destination	Sets the destination of the IP tunnel.
interface tunnel	Creates the IP tunnel.
show interface tunnel	Displays information about the traffic about the specified tunnel interface.

tunnel source

To configure the source endpoint for a tunnel, use the **tunnel source** command. To remove the tunnel source, use the **no** form of this command.

```
tunnel source {ip-address | interface-type number}
no tunnel source [{ip-address | interface-type number}]
```

Syntax Description

<i>ip-address</i>	IP address for the tunnel source.
<i>interface-type number</i>	Interface for the tunnel source.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **tunnel source** command to configure the source address for an IP tunnel.

You should not have two tunnels using the same encapsulation mode with the same source and destination address.

This command requires the Enterprise license.

Examples

This example shows how to set the tunnel source:

```
switch(config-if)# tunnel source 192.0.2.120
```

Related Commands

Command	Description
tunnel destination	Sets the destination of the IP tunnel.
interface tunnel	Creates the IP tunnel.
show interface tunnel	Displays information about the traffic about the specified tunnel interface.

tunnel ttl

To configure the time-to-live value for a tunnel, use the **tunnel ttl** command. To restore the default value, use the **no** form of this command.

tunnel ttl value
no tunnel ttl [value]

Syntax Description

<i>value</i>	Time-to-live value for the tunnel. The range is from 1 to 255.
--------------	--

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Use the **tunnel ttl** command to configure the time-to-live value for an IP tunnel.

This command requires the Enterprise license.

Examples

This example shows how to configure the time-to-live value for a tunnel interface:

```
switch(config-if) # tunnel ttl 30
```

Related Commands

Command	Description
tunnel destination	Sets the destination of the IP tunnel.
interface tunnel	Creates the IP tunnel.
show interface tunnel	Displays information about the traffic about the specified tunnel interface.

tunnel use-vrf

To specify which virtual routing and forwarding (VRF) instance to use to look up a tunnel destination IP address, use the **tunnel use-vrf** command. To return to the default, use the **no** form of this command.

tunnel use-vrf vrf-name
no tunnel use-vrf vrf-name

Syntax Description

<i>vrf-name</i>	Name of the VRF in which to look up the tunnel destination IP address.
-----------------	--

Command Default

Default VRF

Command Modes

Interface configuration mode

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

You should have the tunnel interface and tunnel destination IP address in the same VRF. You should have the same value for the *vrf-name* parameter in both the **vrf member** and **tunnel use-vrf** command.

This command requires the Enterprise license.

Examples

This example shows how to specify the VRF in which to look up the tunnel destination IP address:

```
switch(config-if)# tunnel use-vrf blue
```

Related Commands

Command	Description
show interface tunnel	Displays information about the traffic about the specified tunnel interface.
show vrf interface tunnel	Displays information about the VRF tunnel interface.



U Commands

- [udld](#), on page 336
- [udld aggressive](#), on page 337
- [udld message-time](#), on page 338
- [udld reset](#), on page 339
- [uni-directional link-fault](#), on page 340

udld

To configure the interfaces to use a Unidirectional Link Detection (UDLD) mode, use the **udld** command.

udld {**enable** | **disable**}

Syntax Description

disable	Disables the UDLD mode for fiber interfaces.
enable	Enables the normal UDLD mode for nonfiber interfaces.

Command Default

By default, UDLD is disabled for the 48-port, 10/100/1000-Ethernet module ports.

By default, UDLD is enabled for the 32-port, 10-Gigabit Ethernet module ports.

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Before you can enable a UDLD mode for specified interfaces, you must make sure that UDLD is already enabled globally on the device. Use the **feature udld** command to enable UDLD globally.

Use the **udld** command to enable or disable UDLD separately on specified interfaces . This action enables UDLD in normal mode. Enter the **udld aggressive** command to enable the aggressive mode on UDLD-enabled interfaces.

This command does not require a license.

Examples

This example shows how to enable the normal UDLD mode for Ethernet port 3/1:

```
switch# configure terminal
switch(config)# feature udld
switch(config)# interface ethernet 3/1
switch(config-if)# udld enable
```

This example shows how to disable UDLD for Ethernet port 3/1:

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if-range)# udld disable
```

Related Commands

Command	Description
feature udld	Enables UDLD globally on the device.
show udld	Displays information about the UDLD configuration.

udld aggressive

To configure the interfaces for aggressive Unidirectional Link Detection (UDLD) mode, use the **udld aggressive** command.

udld aggressive

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Interface configuration mode
Global configuration mode

Command History	Release	Modification
	4.0	This command was introduced.

Usage Guidelines Before you can enable the aggressive UDLD mode for an interface, you must make sure that UDLD is already enabled globally on the device and on the specified interfaces.

Use the **udld aggressive** command to configure the ports to use a UDLD mode:

- To enable fiber interfaces for the aggressive mode, enter the **udld aggressive** command in the global command mode and all the fiber interfaces will be in aggressive UDLD mode.
- To enable the copper interfaces for the aggressive, you must enter the **udld aggressive** command in the interface mode, specifying each interface you want in aggressive UDLD mode.

To use the aggressive UDLD mode, you must configure the interfaces on both ends of the link for the aggressive UDLD mode.

This command does not require a license.

Examples

This example shows how to enable fiber interfaces for the aggressive UDLD mode:

```
switch# configure terminal
switch(config)# udld aggressive
```

This example shows how to enable the aggressive UDLD mode for the copper Ethernet interface 3/1:

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# udld aggressive
```

Related Commands

Command	Description
feature udld	Enables UDLD globally for the device.
show udld	Displays information about the UDLD configuration.

udld message-time

To set the Unidirectional Link Detection (UDLD) message interval timer, use the **udld message-time** command.

udld message-time seconds

Syntax Description

<i>seconds</i>	Number of seconds that you want between sending UDLD messages. The range is from 7 to 90 seconds.
----------------	---

Command Default

15 seconds

Command Modes

Global configuration mode

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

Before you can set the UDLD message timer, you must make sure that UDLD is already enabled globally on the device. Use the **feature udld** command to globally enable UDLD.

This command does not require a license.

Examples

This example shows how to configure UDLD interval to 30 seconds:

```
switch# configure terminal
switch(config)# udld message-time 30
```

Related Commands

Command	Description
feature udld	Enables UDLD globally for the device.
show udld	Displays information about the UDLD configuration.

udld reset

To reset the interfaces that Unidirectional Link Detection (UDLD) has shut down and return them to the UP condition, use the **udld reset** command.

udld reset

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Global configuration mode

Release	Modification
4.0	This command was introduced.

Usage Guidelines This command does not require a license.

Examples

This example shows how to reset those interfaces that UDLD has shut down:

```
switch# configure terminal  
switch(config)# udld reset
```

Command	Description
feature udld	Enables UDLD globally for the device.
show udld	Displays information about the UDLD configuration.

uni-directional link-fault

To configure what action is taken on an interface when a link-fault notification is received from the remote Ethernet OAM peer, use the **uni-directional link-fault** command in Ethernet OAM action configuration mode or interface Ethernet OAM action configuration mode. To remove the configuration, use the **no** form of this command.

uni-directional link-fault {**disable** | **efd** | **error-disable-interface** | **log**}
nouni-directional link-fault {**disable** | **efd** | **error-disable-interface** | **log**}

Syntax Description	Parameter	Description
	disable	Performs no action on the interface when a link-fault notification is received.
	efd	Puts the line protocol into the down state for an interface when a link-fault notification is received.
	error-disable-interface	Puts the interface into the error-disable state when a link-fault notification is received.
	log	(Interface Ethernet OAM action configuration only) Creates a syslog entry when a link-fault notification is received. This action is available in Interface Ethernet OAM action configuration mode to override the profile setting and log the event for the interface when it occurs.

Command Default The default action is to create a syslog entry.

Command Modes Ethernet OAM action configuration (config-eoam-action)
 Interface Ethernet OAM action configuration (config-if-eoam-action)

Command History	Release	Modification
	7.3(0)D1(1)	This command was introduced.

Usage Guidelines This command does not require a license.

The following example shows how to configure that no action is performed on the interface when a link-fault notification is received:

```
switch# configure terminal
switch(config)# ethernet oam profile Profile_1
switch(config-eoam)# action
switch(config-eoam-action)# uni-directional link-fault disable
```

The following example shows how to configure putting the interface into the line-protocol-down state when a link-fault notification is received:

```
switch# configure terminal
switch(config)# ethernet oam profile Profile_1
switch(config-eoam)# action
switch(config-eoam-action)# uni-directional link-fault efd
```

The following example shows how to configure that the interface is put into the error-disable state when a link-fault notification is received:

```

switch# configure terminal
switch(config)# ethernet oam profile Profile_1
switch(config-eoam)# action
switch(config-eoam-action)# uni-directional link-fault error-disable-interface

```

The following example shows how to configure that a syslog is created when a link-fault notification is received:

```

switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ethernet oam
switch(config-if-eoam)# action
switch(config-if-eoam-action)# uni-directional link-fault log

```

Related Commands

Command	Description
ethernet oam profile	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM)	Attaches an Ethernet OAM profile to an interface.



V Commands

- [vlan dot1q tag native, on page 344](#)
- [vpc, on page 346](#)
- [vpc config-sync re-merge, on page 347](#)
- [vpc domain, on page 349](#)
- [vpc orphan-ports suspend, on page 350](#)
- [vpc peer-link, on page 351](#)
- [vpc sync, on page 352](#)

vlan dot1q tag native

To enable dot1q (IEEE 802.1Q) tagging for the native VLAN in a trunk, use the **vlan dot1q tag native** command. To return to the default where no packets are tagged in the native VLAN in a trunk, use the **no** form of this command.

```
vlan dot1q tag native [exclude control]
no vlan dot1q tag native [exclude control]
```

Syntax Description	exclude control	Excludes untagged control traffic on the native VLAN in a trunk.
--------------------	-----------------	--

Command Default Disabled

Command Modes Global configuration mode

Command History	Release	Modification
	6.2(10)	The exclude control keyword was added.
	4.0	This command was introduced.

Usage Guidelines Typically, you configure 802.1Q trunks with a native VLAN ID, which strips tagging from all packets on that VLAN and allows all untagged traffic and control traffic to transit the switch. Packets that enter the switch with 802.1Q tags that match the native VLAN ID value are similarly stripped of tagging. If you choose to maintain the tagging on the native VLAN and drop untagged traffic, enter the **vlan dot1q tag native** command.

Use the **vlan dot1q tag native** command to configure the switch to tag the traffic received on the native VLAN and to admit only the 802.1Q-tagged frame, dropping any untagged traffic, including untagged traffic in the native VLAN. Control traffic continues to be accepted untagged on the native VLAN on a trunked port, when the **vlan dot1q tag native** command is enabled.



Note If you enable 802.1Q tagging on one switch and disable it on another switch, all traffic is dropped; you must identically configure 802.1Q tagging on each switch.

To exclude untagged control traffic but include tagged data traffic, use the **vlan dot1q tag native exclude control** command.

The **no vlan dot1q tag native exclude control** command specifies that both control and data traffic will egress the trunk port as untagged.



Note The **vlan dot1q tag native** command applies only to trunk ports.

This command does not require a license.

Examples

This example shows how to enable dot1q tagging for all VLANs on all trunk ports on the switch:

```
switch(config)# vlan dot1q tag native
```

This example shows how to exclude untagged control traffic, but include tagged data traffic for all VLANs on all trunk ports on the switch:

```
switch(config)# vlan dot1q tag native exclude control
```

Related Commands

Command	Description
show vlan dot1q tag native	Displays native VLAN-tagging information.

vpc

To move other port channels into the virtual port channel (vPC), use the **vpc** command. To remove a port channel from the vPC, use the **no** form of this command.

vpc *number*
no vpc *number*

Syntax Description

<i>number</i>	Number for the vPC . The range is from 1 to 4096.
---------------	---

Command Default

None

Command Modes

Interface command mode

Command History

Release	Modification
4.1(3)	This command was introduced.

Usage Guidelines

You must enable the vPC feature before you can create a vPC.

Once you have created the vPC domain ID and the vPC peer link, you create port channels to attach the downstream device to each vPC peer device. That is, you create one port channel from the downstream device to the primary vPC peer device and you create another port channel from the downstream device to the secondary peer device. Finally, working on each vPC peer device, you assign a vPC number to the port channel that connects to the downstream device. You will experience minimal traffic disruption when you are creating vPCs.



Note

The vPC number that you assign to the port channel connecting to the downstream device from the vPC peer device *must* be identical on *both* vPC peer devices.

This command does not require a license.

Examples

This example shows how to move a port channel into the vPC:

```
switch# configure terminal
switch (config)# interface port-channel 10
switch (config-if)# vpc 100
```

Related Commands

Command	Description
show vpc brief	Displays information about vPCs. If the feature is not enabled, the system displays an error when you enter this command.

vpc config-sync re-merge

To enable configuration synchronization between virtual port channel (vPC) peer switches if the current state is not synchronized, use the **vpc config-sync re-merge** command. To undo this configuration, use the **no** form of this command.

vpc config-sync re-merge sync
no vpc config-sync re-merge sync

Syntax Description		
interface ethernet <i>slot/port</i>		Enables the configuration remerge on the specified vPC physical port.
port-channel <i>channel-number</i>		Enables the configuration remerge on the specified port channel.
sync export		Enables the primary switch configuration to be exported to the secondary switch.
sync import		Enables the enables the secondary switch configuration to be imported to primary switch.

Command Default Disabled.

Command Modes Global configuration mode

Command History	Release	Modification
	7.1(1)D1(0)	This command was introduced.

Usage Guidelines Use the **vpc config-sync re-merge** command if the current state of the configuration is not synchronized. The options are as follows:

- Use the **vpc config-sync re-merge sync {export | import}** command to synchronize the configuration with the peer switch.
- Use the **vpc config-sync re-merge sync interface ethernet *slot/port* {export | import}** command to synchronize the physical port configuration.
- Use the **vpc config-sync re-merge sync port-channel *channel-number* {export | import}** command to synchronize the port channel configuration.

This command does not require a license.

Examples

This example shows how to enable configuration synchronization between vPC peer switches. Using the sync export keywords enables the primary switch configuration to be exported to the secondary switch:

```
switch# configure terminal
switch(config)# vpc config-sync re-merge sync export
```

Related Commands

Command	Description
config-sync	Enables vPC configuration synchronization.

vpc domain

To create a virtual port-channel (vPC) domain, use the **vpc domain** command. To remove a vPC domain, use the **no** form of this command.

vpc domain *domain-id*
no vpc domain *domain-id*

Syntax Description	<i>domain-id</i> Domain ID for the vPC . The range of numbers is from 1 to 1000. You must use unique vPC IDs for each vPC within a single virtual device context (VDC).
---------------------------	---

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	4.1(3)	This command was introduced.

Usage Guidelines You must enable the vPC feature before you can create a vPC domain.

You put all vPC interfaces, including the vPC peer link, on both of the vPC peer devices into the identical vPC domain. You must have unique vPC domain numbers within each VDC. In Cisco NX-OS Release 4.1(3), you can have only one vPC per VDC. Once you create a vPC domain, the system automatically creates a vPC system MAC address that is unique to that vPC.

You also use this command to enter the vpc-domain command mode in order to configure vPC parameters.

This command does not require a license.

Examples

This example shows how to create a vPC domain:

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)#
```

This example shows how to enter the vpc-domain command mode to configure an existing vPC domain:

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)#
```

Related Commands	Command	Description
	show vpc brief	Displays information about vPCs. If the feature is not enabled, the system displays an error when you enter this command.

vpc orphan-ports suspend

To suspend a vPC orphan port along with vPC ports, use the **vpc orphan-ports suspend** command in interface-configuration mode. Use the **no** form of this command to revert to default settings.

vpc orphan-ports suspend
no vpc orphan-ports suspend

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Interface configuration mode (config-if)

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines You can use the **vpc orphan-ports suspend** command only on physical ports.



Note You can configure vPC orphan port suspension only on physical ports, not on port channel member ports.

The term “orphaned ports” refers to switch ports connected to single-attached hosts, or vPC ports whose members are all connected to a single vPC peer in a vPC VLAN. End-host can either be attached to a single vPC switch or connected to a vPC pair of switches in an active-standby mode with orphan ports. When a vPC peer-link goes down, while the peer-keepalive link is up, vPC secondary switch suspends all its vPC ports. All the interface VLANs for the vPC VLAN are also brought down during this process. However, orphan ports attached to the vPC secondary switch are not suspended. This may cause traffic disruption for the hosts connected to orphan ports as there is no Layer 3 connectivity for end host through the secondary switch. To suspend the vPC orphan ports along with the vPC ports, use the **vpc orphan-ports suspend** command in interface-configuration mode. The vpc orphan-ports suspend command can be configured on an orphan port that needs to be disconnected from the secondary-operational switch when the vPC peer-link fails.

This command does not require a license.

Examples This example shows how to shut down the vPC port when the peer link is down:

```
switch# configure terminal switch(config)# interface ethernet 5/2
switch(config-if)# vpc orphan-ports suspend
```

Command	Description
vpc domain	Creates a vPC domain.
dual-active exclude interface-vlan	Ensures that specified VLAN interfaces do not go down on the vPC secondary device when the vPC peer link fails.

vpc peer-link

To create a virtual port-channel (vPC) peer link, use the **vpc peer-link** command. To remove a vPC peer link, use the **no** form of this command.

vpc peer-link
no vpc peer-link

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Interface command mode

Command History	Release	Modification
	4.1(3)	This command was introduced.

Usage Guidelines You must enable the vPC feature before you can create a vPC peer link.

You configure a port channel using 10-Gigabit Ethernet ports on the N7K-M132XP-12 module. We recommend that you use the 10-Gigabit Ethernet ports for the channel in dedicated mode and configure at least two of these ports on two different modules into the port channel for redundancy.

Use the **vpc peer-link** command to make that port channel a vPC peer link. The system returns an error message if you attempt to configure a 1-Gigabit Ethernet interface as a vPC peer link.

After you configure the vPC peer device and the vPC peer link is established, the system creates a new MAC address for the vPC and decides which vPC device is the primary device and which is the secondary device.

This command does not require a license.

Examples

This example shows how to create a vPC peer link:

```
switch# configure terminal
switch(config)# interface port-channel 20
switch(config-if)# vpc peer-link
switch(config-vpc-domain)#
```

Related Commands	Command	Description
	show vpc brief	Displays information about vPCs. If the feature is not enabled, the system displays an error when you enter this command.

vpc sync

To synchronize the interface configurations between peer virtual port channels (vPC) devices, use the **vpc sync** command. To undo this configuration, use the **no** form of this command.

```
vpc number sync {export | import}
no vpc number sync {export | import}
```

Syntax Description

export	Enables the primary switch configuration to be exported to the secondary switch.
import	Enables the secondary switch configuration to be imported to the primary switch.

Command Default

Disabled.

Command Modes

Interface configuration mode

Command History

Release	Modification
7.1(1)D1(0)	This command was introduced.

Usage Guidelines

The **vpc sync** command triggers a configuration merge between the primary and secondary switches if the current merge state is failed (for example, there is an interface configuration conflict between the port channels).

This command does not require a license.

Examples

This example shows how to enable configuration synchronization on the vPC physical port on the primary and the secondary switches:

```
switch# configure terminal
switch(config)# interface eth1/1
switch(config-if)# vpc 100
switch(config-if)# vpc 100 sync export
```

Related Commands

Command	Description
show vpc brief	Displays information about vPCs.
vpc	Moves other port channels into the vPC.



W Commands

- [wiring-conflict](#), on page 354

wiring-conflict

To configure what action is taken on an interface when a wiring-conflict event occurs, use the **wiring-conflict** command in Ethernet OAM action configuration mode or interface Ethernet OAM action configuration mode. To remove the configuration, use the **no** form of this command.

```
wiring-conflict {disable | efd | error-disable-interface | log}
no wiring-conflict {disable | efd | error-disable-interface | log}
```

Syntax Description	Parameter	Description
	disable	Performs no action on the interface when a wiring-conflict event occurs.
	efd	Puts the line protocol into the down state for an interface when a wiring-conflict event occurs. The state is removed when the first packet is received without a conflict.
	error-disable-interface	(Interface Ethernet OAM action configuration only) Overrides the profile setting and put the interface into error-disable state when a wiring-conflict event occurs.
	log	Creates a syslog entry when a wiring-conflict event occurs.

Command Default The default action is to put the interface into error-disable state.

Command Modes Ethernet OAM action configuration (config-eoam-action)
Interface Ethernet OAM action configuration (config-if-eoam-action)

Supported User Roles

network-admin
vdc---admin
network---operator
vdc-operator

Command History	Release	Modification
	7.3(0)D1(1)	This command was introduced.

Usage Guidelines This command does not require a license.

The following example shows how to configure that no action is performed on the interface when a wiring-conflict event occurs:

```
switch# configure terminal
switch(config)# ethernet oam profile Profile_1
switch(config-eoam)# action
switch(config-eoam-action)# wiring-conflict disable
```

The following example shows how to configure putting the interface into the line-protocol-down state when a wiring-conflict event occurs:

```
switch# configure terminal
switch(config)# ethernet oam profile Profile_1
switch(config-eoam)# action
switch(config-eoam-action)# wiring-conflict efd
```

The following example shows how to configure that an interface is put into error-disable state when a wiring-conflict event occurs:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ethernet oam
switch(config-if-eoam)# action
switch(config-if-eoam-action)# wiring-conflict error-disable-interface
```

The following example shows how to configure that a syslog entry is created when a wiring-conflict event occurs:

```
switch# configure terminal
switch(config)# ethernet oam profile Profile_1
switch(config-eoam)# action
switch(config-eoam-action)# wiring-conflict log
```

Related Commands

Command	Description
ethernet oam profile	Creates an EOAM profile and enters EOAM configuration mode.
ethernet oam	Enables Ethernet Link OAM, with default values, on an interface and enter interface Ethernet OAM configuration mode.
profile (EOAM)	Attaches an Ethernet OAM profile to an interface.

