Cisco Connected Grid Switch Software Configuration Guide, Cisco IOS Release 12.2(58)EY

Publication Date: July 5, 2011

This guide provides configuration information about the software features released in Cisco IOS Release 12.2(58)EY. This software release is supported on the Connected Grid switch devices listed in the section Supported Hardware, page 1. This document should be used in conjunction with the related software documentation the supported devices

Tell Us What You Think

Send your feedback about this document directly to the Connected Grid Documentation Team.

Connected Grid Documentation Feedback Form

Supported Hardware

Supported Hardware	Hardware Minimum Software Release	Related Software Documentation
Cisco CGS 2520 Switch	Cisco IOS Release 12.2(53)EX	Cisco 2500 Series Connected Grid Switches Configuration Guides

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Cisco IOS Release 12.2(58)EY Features

The following are the software features described in this guide:

IEEE 1588 Precision Time Protocol

This section describes Precision Time Protocol (PTP) and how to configure it on the switch. This section includes following topics:

About Precision Time Protocol

Precision Time Protocol (PTP) is defined in IEEE-1588 as Precision Clock Synchronization for Networked Measurements and Control Systems, and was developed to synchronize the clocks in packet-based networks that include distributed device clocks of varying precision and stability. PTP is designed specifically for industrial, networked measurement and control systems, and is optimal for use in distributed systems because it requires minimal bandwidth and little overhead processing.

Note The section About Precision Time Protocol, page 2, is a general discussion of PTP and PTP profiles. If you are familiar with PTP and PTP profiles, you can skip to the section Configuring PTP on the Switch, page 10, which describes the switch default PTP configuration and how to configure the switch PTP options.

Why PTP?

Smart grid power automation applications such as peak-hour billing, virtual power generators, and outage monitoring and management, require extremely precise time accuracy and stability. Timing precision improves network monitoring accuracy and troubleshooting ability.

In addition to providing time accuracy and synchronization, the PTP message-based protocol can be implemented on packet-based networks, such as Ethernet networks. The benefits of using PTP in an Ethernet network include:

- Low cost and easy setup in existing Ethernet networks
- Very little network bandwidth is needed for PTP data packets

Ethernet Switches and Delays

In an Ethernet network, switches provide a full-duplex communication path between network devices. Switches send data packets to packet destinations using address information contained in the packets. When the switch attempts to send multiple packets simultaneously, some of the packets are buffered by the switch so that they are not lost before they are sent. When the buffer is full, the switch delays sending packets. This delay can cause device clocks on the network lose synchronization with one another.

Additional delays can occur when packets entering a switch are stored in local memory while the switch searches the MAC address table to verify packet CRC fields. This process causes variations in packet forwarding time latency, and these variations can result in asymmetrical packet delay times.

Adding PTP to a network can compensate for these latency and delay problems by correctly adjusting device clocks so that they stay synchronized with one another. PTP enables network switches to function as PTP devices, including boundary clocks and transparent clocks.

Note To learn more about PTP clock devices and their role in a PTP network, refer to the section PTP Clocks, page 7.

Message-Based Synchronization

To ensure clock synchronization, PTP requires an accurate measurement of the communication path delay between the time source (*master*) and the receiver (*slave*). PTP sends messages between the master and slave device to determine the delay measurement. Then PTP measures the exact message transmit time and receive times and uses these times to calculate the communication path delay. PTP then adjusts current time information contained in network data for the calculated delay, resulting in more accurate time information.

This delay measurement principle determines path delay between devices on the network and the local clocks are adjusted for this delay using a series of messages sent between masters and slaves. The one-way delay time is calculated by averaging the path delay of the transmit and receive messages. This calculation assumes a symmetrical communication path; however, switched networks do not necessarily have symmetrical communication paths, due to the buffering process.

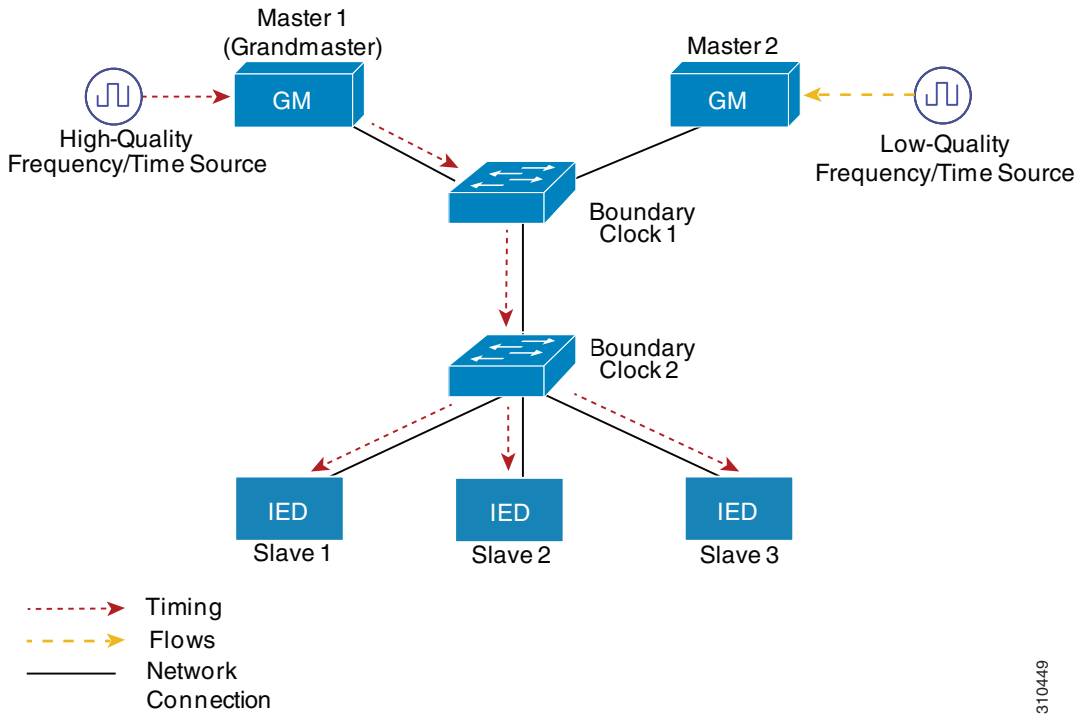
PTP provides a method, using transparent clocks, to measure and account for the delay in a time-interval field in network timing packets, making the switches temporarily transparent to the master and slave nodes on the network. An end-to-end transparent clock forwards all messages on the network in the same way that a switch does.

More Information

- To read a detailed description of synchronization messages, refer to the section PTP Event Message Sequences, page 4.
- To learn more about how transparent clocks calculate network delays, refer to the section Transparent Clock, page 7

Figure 1 shows a typical 1588 PTP network that includes grandmaster clocks, switches in boundary clock mode, and Intelligent Electronic Device (IEDs) such as a digital relays or protection devices. In this diagram, Master 1 is the grandmaster clock. If Master 1 becomes unavailable, the boundary clock slaves switch to Master 2 for synchronization.

Figure 1 PTP Network



PTP Event Message Sequences

This section describes the PTP event message sequences that occur during synchronization.

Synchronizing with Boundary Clocks

The ordinary and boundary clocks configured for the delay request-response mechanism use the following event messages to generate and communicate timing information:

- Sync
- Delay_Req
- Follow_Up
- Delay_Resp

These messages are sent in the following sequence:

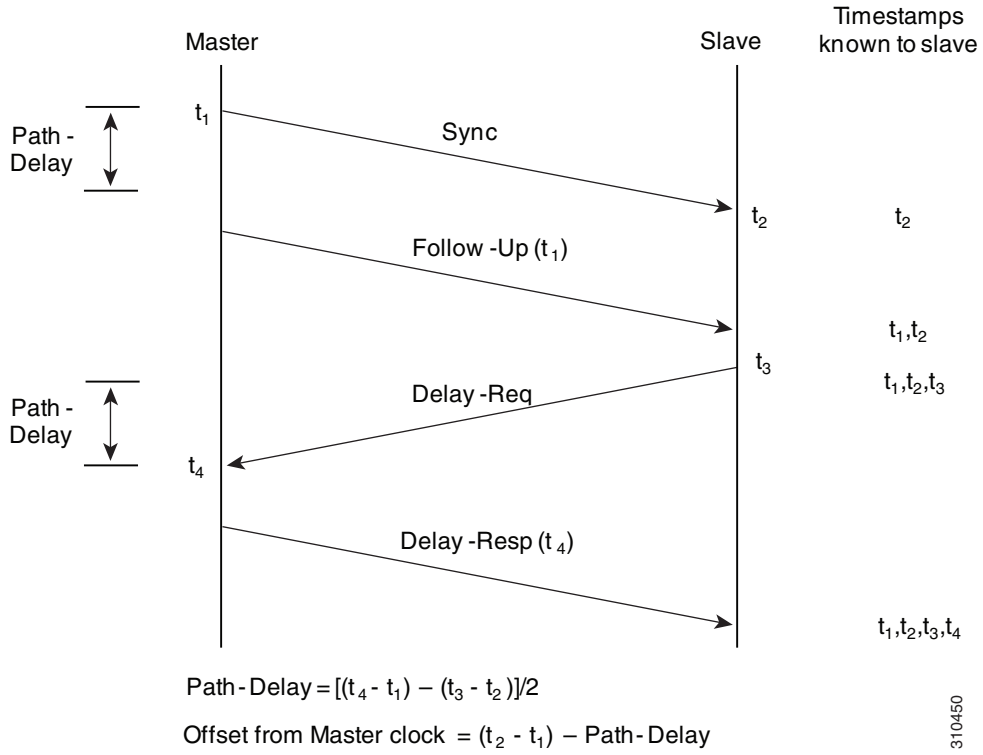
1. The master sends a Sync message to the slave and notes the time (t1) at which it was sent.
2. The slave receives the Sync message and notes the time of reception (t2).
3. The master conveys to the slave the timestamp t1 by embedding the timestamp t1 in a Follow_Up message.
4. The slave sends a Delay_Req message to the master and notes the time (t3) at which it was sent.
5. The master receives the Delay_Req message and notes the time of reception (t4).

6. The master conveys to the slave the timestamp t4 by embedding it in a Delay_Resp message.

After this sequence, the slave possesses all four timestamps. These timestamps can be used to compute the offset of the slave clock relative to the master, and the mean propagation time of messages between the two clocks.

The offset calculation is based on the assumption that the time for the message to propagate from master to slave is the same as the time required from slave to master. This assumption is not always valid on an Ethernet network, due to asymmetrical packet delay times.

Figure 2 Detailed Steps—Boundary Clock Synchronization



Synchronizing with Peer-to-Peer Transparent Clocks

When the network includes multiple levels of boundary clocks in the hierarchy, with non-PTP enabled devices between them, synchronization accuracy decreases.

The round-trip time is assumed to be equal to mean_path_delay/2, however this is not always valid for Ethernet networks. To improve accuracy, the resident time of each intermediary clock is added to the offset in the end-to-end transparent clock. Resident time, however, does not take into consideration the link delay between peers, which is handled by peer-to-peer transparent clocks.

Peer-to-peer transparent clocks measure the link delay between two clock ports implementing the peer delay mechanism. The link delay is used to correct timing information in Sync and Follow_Up messages.

Peer-to-peer transparent clocks use the following event messages:

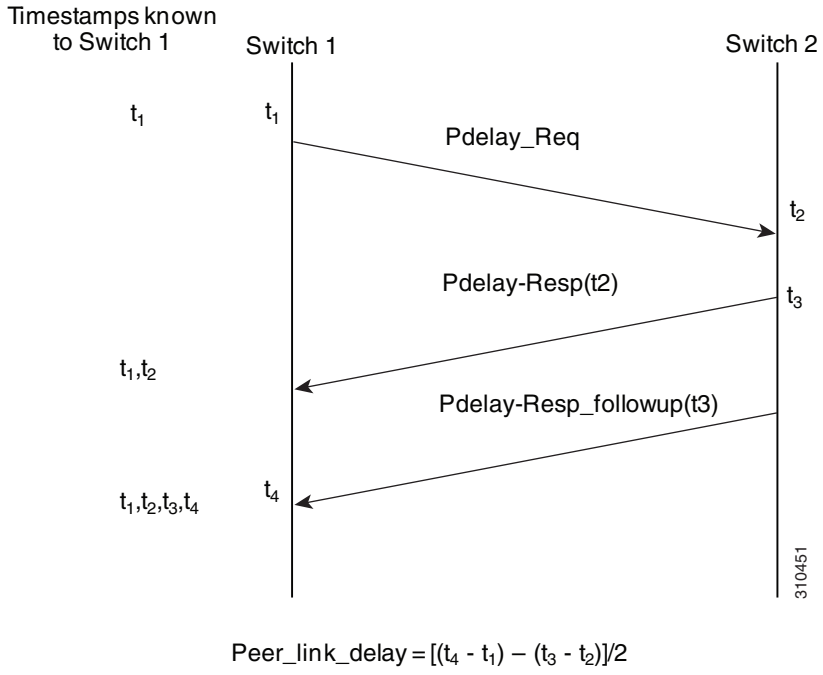
- Pdelay_Req
- Pdelay_Resp
- Pdelay_Resp_Follow_Up

These messages are sent in the following sequence:

1. Port 1 generates timestamp t1 for a Pdelay_Req message.
2. Port 2 receives and generates timestamp t2 for this message.
3. Port 2 returns and generates timestamp t3 for a Pdelay_Resp message.

   To minimize errors due to any frequency offset between the two ports, Port 2 returns the Pdelay_Resp message as quickly as possible after the receipt of the Pdelay_Req message.
4. Port 2 returns timestamps t2 and t3 in the Pdelay_Resp and Pdelay_Resp_Follow_Up messages respectively.
5. Port 1 generates timestamp t4 after receiving the Pdelay_Resp message. Port 1 then uses the four timestamps (t1, t2, t3, and t4) to calculate the mean link delay.

Figure 3 Detailed Steps—Peer-to-Peer Transparent Clock Synchronization



Synchronizing the Local Clock

In an ideal PTP network, the master and slave clock operate at the same frequency. However, *drift* can occur on the network. Drift is the frequency difference between the master and slave clock. You can compensate for drift by using the time stamp information in the device hardware and follow-up messages (intercepted by the switch) to adjust the frequency of the local clock to match the frequency of the master clock.

Best Master Clock Algorithm

The Best Master Clock (BMC) algorithm is the basis of PTP functionality. BMC specifies how each clock on the network determines the best master clock in its subdomain of all the clocks it can see, including itself. The BMC algorithm runs on the network continuously and quickly adjusts for changes in network configuration.

BMC uses the following criteria to determine the best master clock in the subdomain:

- Clock quality (for example, GPS is considered the highest quality)
- Clock accuracy of the clock's time base
- Stability of the local oscillator
- Closest clock to the grandmaster

In addition to identifying the best master clock, BMC also ensures that clock conflicts do not occur on the PTP network by ensuring that:

- Clocks do not have to negotiate with one another
- There is no misconfiguration, such as two master clocks or no master clocks, as a result of the master clock identification process

PTP Clocks

A PTP network is made up of PTP-enabled devices and devices that are not using PTP. The PTP-enabled devices typically consist of the following clock types, which are described in this section:

- Grandmaster Clock, page 7
- Ordinary Clock, page 7
- Boundary Clock, page 7
- Transparent Clock, page 7

Grandmaster Clock

Within a PTP domain, the grandmaster clock is the primary source of time for clock synchronization using PTP. The grandmaster clock usually has a very precise time source, such as a GPS or atomic clock. When the network does not require any external time reference and only needs to be synchronized internally, the grandmaster clock can free run.

Ordinary Clock

An ordinary clock is a PTP clock with a single PTP port. It functions as a node in a PTP network and can be selected by BMC as a master or slave within a subdomain. Ordinary clocks are the most common clock type on a PTP network because they are used as end nodes on a network that is connected to devices requiring synchronization. Ordinary clocks have various interface to external devices.

Boundary Clock

A boundary clock in a PTP network operates in place of a standard network switch or router. Boundary clocks have more than one PTP port, and each port provides access to a separate PTP communication path. Boundary clocks provide an interface between PTP domains. They intercept and process all PTP messages, and pass all other network traffic. The boundary clock uses the BMC algorithm to select the best clock seen by any port. The selected port is then set as a slave. The master port synchronizes the clocks connected downstream, while the slave port synchronizes with the upstream master clock.

Transparent Clock

The role of transparent clocks in a PTP network is to update the time-interval field that is part of the PTP event message. This update compensates for switch delay and has an accuracy of within one picosecond.

There are two types of transparent clocks:

End-to-end (E2E) transparent clocks measure the PTP event message transit time (also known as *resident time*) for SYNC and DELAY_REQUEST messages. This measured transit time is added to a data field (*correction field*) in the corresponding messages:

- The measured transit time of a SYNC message is added to the correction field of the corresponding SYNC or the FOLLOW_UP message.
- The measured transit time of a DELAY_REQUEST message is added to the correction field of the corresponding DELAY_RESPONSE message.

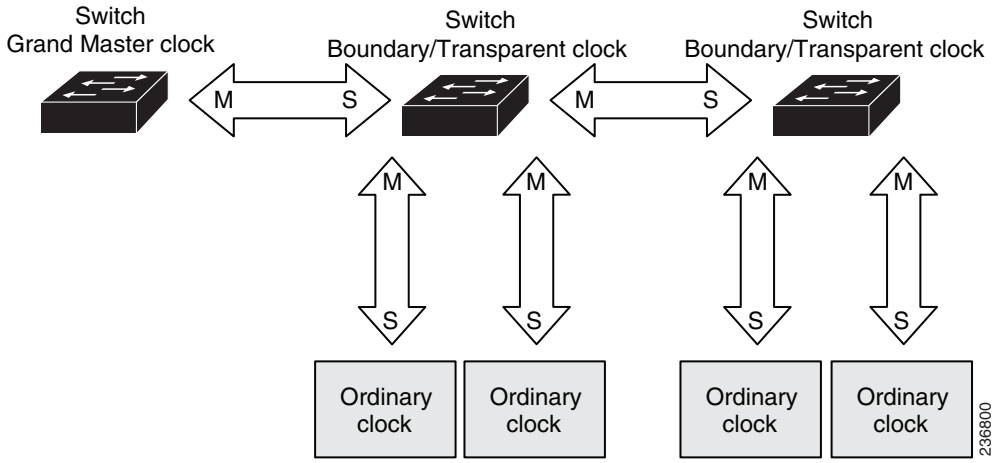
The slave uses this information when determining the offset between the slave's and the master's time. E2E transparent clocks do not provide correction for the propagation delay of the link itself.

Peer-to-peer (P2P) transparent clocks measure PTP event message transit time in the same way E2E transparent clocks do, as described above. In addition, P2P transparent clocks measure the upstream link delay. The upstream link delay is the estimated packet propagation delay between the upstream neighbor P2P transparent clock and the P2P transparent clock under consideration.

These two times (message transit time and upstream link delay time) are both added to the correction field of the PTP event message, and the correction field of the message received by the slave contains the sum of all link delays. In theory this is the total end-to-end delay (from master to slave) of the SYNC packet.

Figure 4 illustrates PTP clocks in a master-slave hierarchy within a PTP network.

Figure 4 PTP Clock Hierarchy



About the PTP Power Profile

This section describes PTP profiles and specifically the PC37.238 IEEE-1588 standard, Power Profile, which is also known as the Profile for Protection Applications.

Note The switch documentation and CLI use the terms Power Profile, power profile mode, and non-power profile mode when referring to this IEEE-1588 profile and its associated configuration values.

What are PTP Profiles?

The IEEE-1588 definition of a PTP profile is *the set of allowed PTP features applicable to a device*. A PTP profile is usually specific to a particular type of application or environment and defines the following values:

- Best master clock algorithm options
- Configuration management options
- Path delay mechanisms (peer delay or delay request-response)
- Range and default values of all PTP configurable attributes and data set members
- Transport mechanisms that are required, permitted, or prohibited
- Node types that are required, permitted, or prohibited
- Options that are required, permitted, or prohibited

Power Profile Description

The IEEE Power Profile defines specific or allowed values for PTP networks used in power substations. The defined values include the optimum physical layer, the higher level protocol for PTP messages, and the preferred best master clock algorithm. The Power Profile values ensure consistent and reliable network time distribution within substations, between substations, and across wide geographic areas.

The switch is optimized for PTP in these ways:

- Hardware— The switch uses a Sprite FPGA, which time stamps the Fast Ethernet and Gigabit Ethernet ports.
- Software—The switch default configuration is power profile mode. In this mode, the switch uses the configuration values defined in the IEEE-1588 Power Profile standard.

Table 1 lists the configuration values defined by the IEEE-1588 Power Profile.

Table 1 Configuration Values for the IEEE PTP Power Profile and Switch Modes

PTP Field	Power Profile Value	Switch Configuration Value	
		Power Profile Mode	**Non-Power Profile Mode**
Message transmission	Ethernet 802.3, with Ethertype 0X88F7. PTP messages are sent as 802.1Q tagged Ethernet frames with a default VLAN 0 and default priority 4.	**Access Ports**–Untagged Layer 2 packets, **Trunk Ports**–802.1Q tagged Layer 2 packets with native VLAN on the port and default priority value of 4.	Layer 3 packets. By default, 802.1q tagging is disabled.
MAC address–Non-peer delay messages	01-1B-19-00-00-00.	01-1B-19-00-00-00.	01-1B-19-00-00-00.
MAC address–Peer delay messages	01-80-C2-00-00-0E.	01-80-C2-00-00-0E.	Not applicable to this mode.
Domain number	0.	0.	0.
Path delay calculation	Peer-to-peer transparent clocks.	Peer-to-peer transparent clocks using the peer_delay mechanism.	End-to-end transparent clocks using the delay_request mechanism.
BMC	Enabled.	Enabled.	Enabled.

PTP Field	Power Profile Value	Switch Configuration Value	
		Power Profile Mode	Non-Power Profile Mode
Clock type	Two-step and one-step clocks are supported. Two-step is preferred for Ethernet.	Two-step.	Two-step.
Time scale	Epoch.[1]	Epoch.	Epoch.
Grandmaster ID and local time determination	PTP-specific TLV (type, length, value) to indicate Grandmaster ID.	PTP-specific TLV to indicate Grandmaster ID.	PTP-specific type, length, and value to indicate Grandmaster ID.
Time accuracy over network hops	Over 16 hops, slave device synchronization accuracy is within 1 usec (1 microsecond).	Over 16 hops, slave device synchronization accuracy is within 1 usec (1 microsecond).	Not applicable in this mode.

1. Epoch = Elapsed time since epoch start.

Configuring PTP on the Switch

This section describes how to configure the switch for PTP applications.

Power Profile Modes on the Switch

This section describes the two PTP modes that the switch uses.

Note For detailed information about the IEEE-1588 Power Profile, refer to About the PTP Power Profile, page 8.

Power Profile Mode

By default, the switch PTP configuration uses the values defined by the IEEE-1588 Power Profile and the switch is in power profile mode. In this mode:

- The PTP mode of transport is Layer 2.
- The supported transparent clock mode is peer-to-peer (P2P).

Table 1 on page 9 lists the configuration values for the switch in power profile mode.

Non-Power Profile Mode

When power profile mode is disabled on the switch with the **no ptp profile power** command, the switch is in non-power profile mode. In this mode:

- The PTP mode of transport is Layer 3.
- The supported transparent clock mode is end-to-end (E2E).

Table 1 on page 9 lists the configuration values for the switch in non-power profile mode.

PTP Clock Modes Supported on the Switch

PTP synchronization behavior depends on the PTP clock mode that you configure on the switch. You can configure the switch for one of the following global modes:

- Boundary Clock Mode
- Forward Mode
- E2E Transparent Clock Mode
- P2P Transparent Clock Mode

Boundary Clock Mode

A switch configured for boundary clock mode participates in selecting the best master clock on the subdomain, selecting from all clocks it can see, including itself. If the switch does not detect a more accurate clock than itself, then the switch becomes the master clock. If a more accurate clock is detected, then the switch synchronizes to that clock and becomes a slave clock.

After initial synchronization, the switch and the connected devices exchange PTP timing messages to correct the changes caused by clock offsets and network delays. These are some guidelines for this mode:

- You can enable this mode when the switch is in Power Profile Mode (Layer 2) or in Non-Power Profile Mode (Layer 3).
- The switch must be in this mode to configure PTP on individual switch ports.

Forward Mode

A switch configured for forward mode passes incoming PTP packets as normal multicast traffic. These are some guidelines for this mode:

- You can enable this mode when the switch is in Power Profile Mode (Layer 2) or in Non-Power Profile Mode (Layer 3).
- When the switch is in this mode, the only PTP configuration available is PTP mode.
- The switch must be in Boundary Clock Mode to configure PTP on individual switch ports.

E2E Transparent Clock Mode

A switch configured for end-to-end transparent clock mode does not synchronize its clock with the master clock. A switch in this mode does not participate in master clock selection and uses the default PTP clock mode on all ports. These are some guidelines for this mode

- You can enable this mode only when the switch is in Non-Power Profile Mode (Layer 3).
- When the switch is in this mode, the only PTP configuration available is PTP mode.
- The switch must be in Boundary Clock Mode to configure PTP on individual switch ports.

P2P Transparent Clock Mode

A switch configured for peer-to-peer transparent clock mode does not synchronize its clock with the master clock. A switch in this mode does not participate in master clock selection and uses the default PTP clock mode on all ports. These are some guidelines for this mode:

- You can enable this mode only when the switch is in Power Profile Mode (Layer 2).
- When the switch is in this mode, the only PTP configuration available is PTP mode.
- The switch must be in Boundary Clock Mode to configure PTP on individual switch ports.

Switch Configuration Guidelines for PTP

Be aware of the guidelines in this section when you configure PTP on the switch.

PTP Mode and Profile Guidelines

- PTP is enabled on the switch by default.
- By default, the switch uses configuration values defined in the PTP Power Profile (power profile mode is enabled).
- The switch default PTP clock mode is P2P Transparent Clock Mode.
- The switch and the grandmaster clock must be in the same PTP domain.
- When power profile mode is enabled, the switch drops the PTP announce messages that do not include these two Type, Length, Value (TLV) message extensions: *Organization_extension* and *Alternate_timescale*.

  If the grandmaster clock is not compliant with PTP and sends announce messages without these TLVs, configure the switch to process the announce message by entering the **ptp allow-without-tlv** command.

  Refer to the section Configuring PTP Power Profile Mode on the Switch, page 13, for a complete description of this command.
- When the switch is in power profile mode, only the peer_delay mechanism is supported.

  To change to Boundary Clock Mode and the peer_delay mechanism, enter the **ptp mode boundary pdelay-req** command.
- To disable power profile mode and return the switch to E2E Transparent Clock Mode, enter the **no ptp profile power** command.

  Refer to the section Configuring Non-Power Profile Mode on the Switch, page 15, for a complete description of this command.
- In non-power profile mode, only the delay_request mechanism is supported.

  To change to Boundary Clock Mode with the delay_request mechanism, enter the **ptp mode boundary delay-req** command.

Packet Format Guidelines

- The packet format for PTP messages can be 802.1q tagged packets or untagged packets.
- The switch does not support 802.1q QinQ Tunneling.
- In switch power profile mode:
  - When the PTP interface is configured as an access port, PTP messages are sent as untagged, Layer 2 packets.
  - When the PTP interface is configured as a trunk port, PTP packets are sent as 802.1q tagged Layer 2 packets over the port native VLAN.
- Slave IEDs must support tagged and untagged packets.
- When PTP packets are sent on the native VLAN in E2E Transparent Clock Mode, they are sent as untagged packets. To configure the switch to send them as tagged packets, enter the global **vlan dot1q tag native** command.

VLAN Configuration Guidelines

- Most grandmaster clocks use the default VLAN 0. In power profile mode, the switch default VLAN is VLAN 1 and VLAN 0 is reserved. When you change the default grandmaster clock VLAN, it must be changed to a VLAN other than 0.
- When VLAN is disabled on the grandmaster clock, the PTP interface must be configured as an access port.

Clock Configuration Guidelines

- The switch FPGA PTP clock only is synchronized to the grandmaster clock. The switch system clock is not synchronized as part of PTP configuration and processes.
- When VLAN is enabled on the grandmaster clock, it must be in the same VLAN as the native VLAN of the PTP port on the switch.
- Grandmaster clocks can drop untagged PTP messages when a VLAN is configured on the grandmaster clock. To force the switch to send tagged packets to the grandmaster clock, enter the global **vlan dot1q tag native** command.

Configuring PTP Power Profile Mode on the Switch

This section describes how to configure the switch to use the PTP Power Profile and operate in power profile mode.

- For complete information about PTP profiles and the Power Profile, refer to the section About the PTP Power Profile, page 8.
- For details about switch power profile mode, refer to the section Power Profile Mode, page 10.

Before You Begin

These are some guidelines for configuring the Power Profile on the switch:

- When you enter **no** with PTP port configuration commands, the specified port property is set to the default value.
- To determine the value in seconds for the **ptp** global command *interval* variable, use a logarithmic scale. Below are examples of the *interval* variable value converted to seconds with a logarithmic scale:

Value Entered	Logarithmic Calculation	Value in Seconds
-1	2^{-1}	1/2
0	2^{0}	1

To configure the switch for power profile mode, follow these steps:

	Command	Description
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**ptp profile power**	Enables the PTP Power Profile on the switch and configures the switch for power profile mode (if the switch is in non-power profile mode). The switch default configuration is power profile enabled. If the switch is already in power profile mode, then this command has no effect.
Step 3	**ptp** {**allow-without-tlv** | **domain** | **mode** {**boundary pdelay-req** | **p2ptransparent** | **forward**} | **packet** | **priority1** *priority* | **priority2** *priority*}	Specifies the synchronization clock mode. • **allow-without-tlv**—Enables PTP message processing for announce messages that do not include the *Organization_extension* and *Alternate_Timescale_ Offset_ Indicato*r TLVs. • **domain**—Sets the PTP clock domain. The participating grandmaster clock, switches, and slave devices should be in the same domain. • **mode boundary pdelay-req**—Configures the switch for boundary clock mode using the peer delay request (pdelay-req) mechanism. A switch in boundary clock mode participates in the selection of the most accurate master clock. The peer_link delay between PTP ports is included in the offset calculation. Use this mode when heavy network conditions produce significant delay jitter. • **mode p2ptransparent**—Default clock mode. Configures the switch for peer-to-peer transparent clock mode and synchronizes all switch ports with the master clock. The link delay time between the participating PTP ports and the message transit time is added to the resident time. Use this mode to reduce jitter and error accumulation. • **mode forward**—Configures the switch to pass incoming PTP packets as normal multicast traffic. The following options specify the clock priority properties when the switch port is in boundary mode. • **packet**—Changes the PTP packet priority. The default is priority 4. Lower values take precedence. • **priority1**—Overrides the default criteria (such as clock quality and clock class) for the most accurate master clock selection. • **priority2**—Breaks the tie between two switches that match the default criteria. For example, enter 2 to give a switch priority over identical switches. • *priority* —A priority number from 0 to 255. The default is 128.
Step 4	**interface** *interface-id*	Enters interface configuration mode.

	Command	Description
Step 5	**ptp** {**announce interval** {*interval*} | **timeout** {*timeout-in-secs*} | **delay-req** {**interval** *interval*} | **enable** | **pdelay-req** {**interval** *interval*} | **sync** {**interval** *interval*} | **limit** {*offset-in-nanosecs*}}	Specifies the settings for PTP timing messages. These options are available only when the switch is in boundary mode. • *interval*—Interval time. You can calculate interval seconds from the value you enter using a logarithmic scale as described in the section Configuring PTP Power Profile Mode on the Switch, page 13. • **announce interval** *interval*—Sets the time to send announce messages. The range is 0 to 4 seconds. The default is 0 seconds (entered value: 0). • **announce timeout** *timeout-in-secs*— Sets the time to announce timeout messages. The range is 2 to 10 seconds. The default is 8 seconds (entered value is 3). • **delay-req interval** *interval*—Sets the time interval for slave devices to send delay request messages when the port is in the master clock state. The range is -1 to 6 seconds. The default is 32 seconds (entered value is 5). • **enable**—Enables PTP on the port base module. • **pdelay-req interval** *interval*—Sets the time interval for PTP devices to send peer_delay request messages when the peer_delay mechanism is enabled. The range is -3 to 5. The default is 0 (0 seconds). • **sync interval** *interval*—Sets the time interval to send synchronization messages. The range is –1 to 1 second. The default is 1 second. • **sync limit** *offset-in-nanosecs*—Sets the maximum clock offset value before PTP attempts to resynchronize. The range is 50 to 500000000 nanoseconds. The default is 500000000 nanoseconds.
Step 6	**end**	Returns to privileged EXEC mode.
Step 7	**show running-config**	Verifies your entries.
Step 8	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

Configuring Non-Power Profile Mode on the Switch

This section describes how to configure the switch to operate in non-power profile mode.

- For complete information about PTP profiles and the Power Profile, refer to the section About the PTP Power Profile, page 8.
- For details about switch non-power profile mode, refer to the section Non-Power Profile Mode, page 10.

Before You Begin

The switch sends untagged PTP packets on the native VLAN when the switch port connected to the grandmaster clock is configured as follows:

- Switch is in non-power profile mode.
- Switch is in trunk mode.
- VLAN X is configured as the native VLAN.

When the grandmaster clock requires tagged packets, make one of the following configuration changes:

- Force the switch to send tagged frames by entering the global **vlan dot1q tag native** command.
- Configure the grandmaster clock to send and receive untagged packets. If you make this configuration change on the grandmaster clock, you can configure the switch port as an access port.

To configure the switch for non-power profile mode, follow these steps:

	Command	Description
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**no ptp profile power**	Configures the switch for non-power profile mode when the switch is in power profile mode. If the switch is already in non-power profile mode, this command has no effect.
Step 3	**ptp** {**domain** | **mode boundary delay-req** | **e2etransparent** | **forward**} | **packet** | **priority1** *priority* | **priority2** *priority*}	Specifies the synchronization clock. • **domain**—Sets the PTP clock domain. The participating grandmaster clock, switches, and slave devices should be in the same domain. • **mode boundary delay-req**—Configures the switch for boundary clock mode using the delay-request mechanism. In this mode, the switch participates in the selection of the most accurate master clock. Use this mode when overload or heavy load conditions produce significant delay jitter. • **mode e2etransparent**—Configures the switch for end-to-end transparent clock mode. A switch clock in this mode synchronizes all switch ports with the master clock. This switch does not participate in master clock selection and uses the default PTP clock mode on all ports. This is the default clock mode. The message transit times is added to the resident time. Use this mode to reduce jitter and error accumulation. • **mode forward**—Configures the switch to pass incoming PTP packets as normal multicast traffic. These options specify the clock priority properties when the switch port is in boundary mode: • **packet**—Changes the PTP packet priority. The PTP packets have a default priority of 4. Lower values take precedence. • **priority1** *priority*—Overrides the default criteria (such as clock quality and clock class) for the most accurate master clock selection. • **priority2** *priority*—Breaks the tie between two switches that match the default criteria. For example, enter 2 to give a switch priority over identical switches. • *priority* —A priority number from 0 to 255. The default is 128.
Step 4	**interface** *interface-id*	Enters interface configuration mode.

	Command	Description
Step 5	**ptp** {**announce** {**interval** *interval* | **timeout** *interval*} | **delay-req interval** *interval* | **enable** | **sync** {**interval** *interval* | **limit** *offset-in-nanosecs*}}	Specifies the settings for the timing messages. These options are available only when the switch is in boundary mode. • *interval*—Interval time. You can calculate interval seconds from the value you enter using a logarithmic scale as described in the section Configuring PTP Power Profile Mode on the Switch, page 13. • **announce interval** *interval*—Sets the time to send announce messages. The range is 0 to 4 seconds. The default is 0 (0 seconds). • **announce timeout** *interval*— Sets the time to announce timeout messages. The range is 2 to 10 seconds. The default is 8 seconds (entered value is 3). • **delay-req interval** *interval*—Sets the time for slave devices to send delay request messages when the port is in the master clock state. The range is -1 second to 6 seconds. The default is 32 seconds (entered value is 5). • **enable**—Enables PTP on the port base module. • **sync interval** *interval*—Sets the time to send synchronization messages. The range is –1 to 1 second. The default is 1 second. • **sync limit** *offset-in-nanosecs*—Sets the maximum clock offset value before PTP attempts to resynchronize. The range is from 50 to 500000000 nanoseconds. The default is 500000000 nanoseconds.
Step 6	**end**	Returns to privileged EXEC mode.
Step 7	**show running-config**	Verifies your entries.
Step 8	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

PTP Show Commands

This section describes the PTP **show** command options.

PTP Show Command Syntax	Description
show ptp {**clock** | **foreign-master-records** | **parent** | **port** {**FastEthernet** | **GigabitEthernet**} | **time property**}	Specifies the PTP information to display. • **clock**—Displays PTP clock information. • **foreign-master-records**—Displays PTP foreign-master-records. • **parent**—Displays PTP parent properties. • **port FastEthernet**—Displays PTP properties for the FastEthernet IEEE 802.3 interfaces. • **port GigabitEthernet**—Displays PTP properties for the GigabitEthernet IEEE 802.3z interfaces. • **time property**—Displays PTP clock-time properties.

Tagging Behavior for PTP Packets

Table 2 describes the switch tagging behavior in power profile and non-power profile modes.

Table 2 Tagging Behavior for PTP Packets

Switch Port Mode	Configuration	Power Profile Mode		Non-Power Profile Mode	
		Behavior	Priority	Behavior	Priority
Trunk Port	**vlan dot1q tag native** enabled	Switch tags packets.	7	Switch tags packets.	7
Trunk Port	**vlan dot1q tag native** disabled	PTP software tags packets.	4	Untagged	None
Access Port	N/A	Untagged	None	Untagged	None

Temperature and Voltage Monitoring

Cisco IOS Release 12.2(28)EY includes enhancements to features that support monitoring of the switch operating temperature and power supply voltage. This section describes how to configure this feature on the switch, and includes the following topics:

Power Supply Voltage Monitoring

Earlier software releases for the switch supported user configurable alarm thresholds (maximum and minimum) for the switch operating temperature. You can configure operating temperature ranges (primary and secondary) for the switch, and then configure alarm options to trigger an event message when the switch operating temperature is out of the defined range.

Cisco IOS Release 12.2(58)EY includes a similar feature for the switch power supply. You can configure power supply voltage ranges and then configure alarm options for when the voltage is out of range. These features include:

- User configurable thresholds for the power supply voltage.
- Support for SNMP traps and SYSLOG messages (alarms) when the power supply voltage exceeds or falls below the configured thresholds.

Historical Data Collection

Cisco IOS Release 12.2(58)EY includes new features to support switch historical data collection and storage. Use these features to configure the switch to save historical data about switch operating temperature and power supply voltage. New features include:

- Historical data collection and storage for temperature and voltage information.

- A **show** command that displays the configuration and historical data for temperature and voltage.
- An enhanced MIB enables historical data retrieval so that network management systems can collect report data from the switch.
- Commands for monitoring redundant power supplies.

Monitoring and Storing Temperature and Voltage Data

This section describes how often the switch monitors and stores temperature and voltage data.

Monitoring Interval

The switch checks the operating temperature and power supply voltage once per minute.

Storage Interval

The switch stores temperature and voltage data as follows:

- Every 60 seconds, the switch stores the actual, measured temperature and voltage.
- Every 60 minutes, the switch stores the average of the 60 measurements taken during the previous hour.

You must enter the **alarm facility history** command to enable the switch to store the data that it collects at the monitoring intervals. Refer to these sections for details about how to use these commands:

- The **alarm facility temperature history** command is described in the section Configure Temperature Monitoring Features, page 20
- The **alarm facility power-supply voltage history** command is described in the section Configure Power Supply Monitoring Features, page 21

Maximum Storage Period

The switch stores temperature and voltage data for a maximum of 72 hours. After 72 hours, the oldest data is purged as the switch adds the most recent data.

Alarms

At each monitoring interval, the switch checks the operating temperature and power supply voltage. If the switch detects that either is out of range of the thresholds defined with the **alarm facility** command, then it generates an event message (alarm). The message type is SYSLOG or SNMP trap. Refer to these sections for details about how to use these commands:

- The **alarm facility temperature** command is described in the section Configure Temperature Monitoring Features, page 20
- The **alarm facility power-supply voltage** command is described in the section Configure Power Supply Monitoring Features, page 21
- The **alarm facility power-supply rps** command is described in the section Configure RPS Monitoring Features, page 23

Configuring Temperature and Voltage Monitoring Options

This section describes the temperature and voltage monitoring configuration commands supported in Cisco IOS Release 12.2(58)EY and later.

Configure Temperature Monitoring Features

Use the **alarm facility temperature** global configuration command to configure temperature thresholds for the purpose of generating event messages (alarms). You can configure an alarm for both of these threshold types.

You can also use this command to:

- Configure the alarm options to use when operating temperature is outside the configured threshold ranges.
- Enable historical data collection for operating temperature ranges.
- Use the **no** form of the command to disable the specified setting
- To reset the high or low paramter to the default value, use the **no** form of the command with the previously entered value, for example:

```
Switch)# no alarm facility temperature primary low 220
```

Command Syntax	Description
alarm facility temperature {history | primary {low *celsius* | high *celsius* | notifies | relay major | syslog} | secondary {low *celsius* | high *celsius* | notifies | syslog} }	The **alarm facility temperature** global command configures the operating temperature thresholds, alarm settings, and historical data settings for the switch. • **history**—Enables historical data collection for the switch operating temperature. The default setting is disabled. • **primary**—Configures the primary temperature thresholds. • **secondary**—Configures the secondary temperature thresholds. • **high *celsius***—Maximum temperature in degrees celsius that, when exceeded, triggers an alarm event on the switch. The range is -150 to 300. The default value is 110. • **low *celsius***—Minimum temperature in degrees celsius that, when not met, triggers an alarm event on the switch. The range is -200 to 250. The default value is -25. • **notifies**—Generates an SNMP trap when the switch operating temperature is out of range of the configured threshold values. The default setting is disabled. • **relay major**—Sends alarms across the major relay circuits. This is the default configuration and it cannot be changed. • **syslog**—Generates a SYSLOG message when the switch operating temperature is out of range of the configured threshold values. The default setting is enabled.

Configure Power Supply Monitoring Features

Supported Power Supplies

The switch supports the power supply models described below. The **alarm facility power-supply voltage** command options and alarm threshold ranges are different for each model.

For detailed information about these power supplies, refer to the switch hardware installation guide.

Power Supply Model	Description	set threshold Command Option	Threshold Ranges
PWR-RGD-AC-DC	High-voltage AC or DC.	**threshold ac-dc**	• High: 275 to 300 volts • Low: 75 to 80 volts
PWR-RGD-LOW-DC	Low-voltage DC.	**threshold low-dc**	• High: 75 to 80 volts • Low: 16 to 20 volts

Use the **alarm facility power-supply voltage** global configuration command to configure voltage thresholds for the purpose of generating event messages (alarms). You can also use this command to:

- Configure the event notification options to use when power supply voltage is outside the configured threshold ranges.
- Enable historical data collection of power supply voltage.
- Use the **no** form of the command to disable the specified setting
- Use the **no** form of the command to reset a parameter to the default value.

Command Syntax	Description
alarm facility power-supply voltage {**disable** | **history** | **notifies** | **relay major**} | **syslog** | **threshold ac-dc** {**high** *volts* | **low** *volts*}| **threshold low-dc** {**high** *volts* | **low** *volts*}}	The **alarm facility power-supply voltage** global configuration command configures the power supply thresholds, alarm settings, and historical data settings for the switch power supplies. • **disable**—Disables threshold alarms for the power supply. • **history**—Enables historical data collection for the power supplies. The default setting is disabled. • **notifies**—Generates an SNMP trap when the power supply voltage exceeds the **high** value or falls below the **low** value. The default setting is disabled. • **relay major**—Sends alarms across the major relay circuits. This is the default setting and it cannot be changed. • **syslog**—Generates a SYSLOG message when the power supply voltage exceeds the **high** value or falls below the **low** value. The default setting is enabled. • **threshold ac-dc**—Configures the maximum and minimum threshold values for the PWR-RGD-AC-DC power supply. • **threshold low-dc**—Configures the maximum and minimum threshold values for the PWR-RGD-LOW-DC power supply. • **high** *volts*—Maximum power supply voltage that, when exceeded, triggers an alarm event on the switch. The range is: – **threshold ac-dc:** 275 to 300 – **threshold low-dc:** 75 to 80 The default values are: – **ac-dc high:** 275 – **low-dc high:** 80 • **low** *volts*—Minimum power supply voltage that, when not met, triggers an alarm event on the switch. The range is: – **threshold ac-dc:** 75 to 85 – **threshold low-dc:** 16 to 20 The default values are: – **ac-dc low:** 80 – **low-dc low:** 17

Configure RPS Monitoring Features

Use the **alarm facility power-supply rps** global configuration command to configure event messages (alarms) for the switch redundant power supply (RPS). Use this command to:

- Configure the relay circuits on which RPS alarms are sent.
- Configure the alarm settings to use for RPS alarms.
- Disable alarms for the RPS.
- Use the **no** form of the command to disable the specified RPS setting.

Command Syntax	Description
alarm facility power-supply rps {disable | relay major | syslog | notifies}	The **alarm facility power-supply rps** global configuration command configures the event message options for the RPS. • **disable**—Disables alarms for the redundant power supply. • **notifies**—Generates an SNMP when the switch operating temperature is out of range of the configured threshold values. • **relay major**—Sends alarms across the major relay circuits. This is the default setting and it cannot be changed. • **syslog**—Generates a SYSLOG message when the switch operating temperature is out of range of the configured threshold values.

Temperature and Voltage Monitoring Show Commands

This section describes the temperature and voltage monitoring **show** commands supported in Cisco IOS Release 12.2(58)EY and later.

Command Syntax	Description
show {**alarm settings | env** {**all | temperature history | power-supply history**}}	The **show** command displays configuration information and historical data for the switch operating temperature and power supply voltage. • **alarm settings**—Displays the power supply temperature configuration. • **env**—Displays historical data for the selected option. • **all**—Displays historical data for the switch operating temperature and the power supply voltage. • **temperature history**—Displays historical data for the switch operating temperature. • **power-supply history**—Displays historical data for the switch power supply voltage.

MIB Support for TVM

This section describes the MIBs that are supported by the TVM feature:

- CISCO-ENTITY-SENSOR-MIB—Collects history information about temperature and power-supply monitoring on the router.
- CISCO-ENTITY-SENSOR-HISTORY-MIB—Provides five objects that support read-write operations:
  - entSensorThresholdSeverity
  - entSensorThresholdRelation
  - entSensorThresholdValue
  - entSensorThresholdNotificationEnable
  - entSensorThreshNotifGlobalEnable

Note TVM supports read operations (get operations) only, including for objects that support read and write operations.

Enable Entity Sensor Threshold Notifications

To enable entity sensor threshold notifications, enter the **snmp-server enable traps entity-sensor threshold** global configuration command. To disable entity sensor threshold notifications, enter the **no** form of this command.

Specify SNMP Notification Recipients

To specify the recipient of an SNMP notification operation for entity sensor threshold, enter the **snmp-server host** global configuration command. To remove the specified host, enter the **no** form of this command.

Bidirectional Forwarding Detection Protocol

The Bidirectional Forwarding Detection (BFD) Protocol quickly detects forwarding-path failures for a variety of media types, encapsulations, topologies, and routing protocols. It operates in a unicast, point-to-point mode on top of any data protocol being forwarded between two systems to track IPv4 connectivity between directly connected neighbors. BFD packets are encapsulated in UDP packets with a destination port number of 3784 or 3785.

BFD over Switched Virtual Interfaces

BFD is supported on physical interfaces that are configured as routing interfaces. Starting with Cisco IOS release 12.2(55)SE, BFD is also supported on Switched Virtual Interfaces (SVIs).

In EIGRP, IS-IS, and OSPF deployments, the closest alternative to BFD is the use of modified failure-detection mechanisms. Although reducing the EIGRP, IS-IS, and OSPF timers can result in a failure-detection rate of 1 to 2 seconds, BFD can provide failure detection in less than 1 second. BFD can be less CPU-intensive than the reduced timers and, because it is not tied to any particular routing protocol, it can be used as a generic and consistent failure detection mechanism for multiple routing protocols.

To create a BFD session, you must configure BFD on both systems (BFD peers). Enabling BFD at the interface and routing protocol level on BFD peers creates a BFD session. BFD timers are negotiated and the BFD peers send control packets to each other at the negotiated intervals. If the neighbor is not directly connected, BFD neighbor registration is rejected.

Figure 1-5 shows a simple network with two routers running OSPF and BFD. When OSPF discovers a neighbor (1), it sends a request to the BFD process to initiate a BFD neighbor session with the neighbor OSPF router (2), establishing the BFD neighbor session (3).

Figure 1-5 Establishing a BFD Session

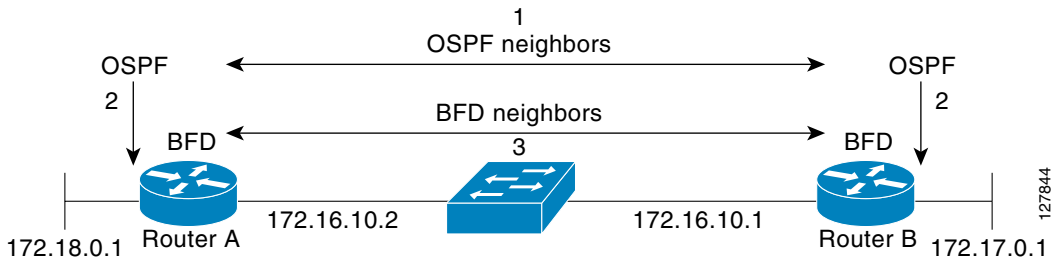
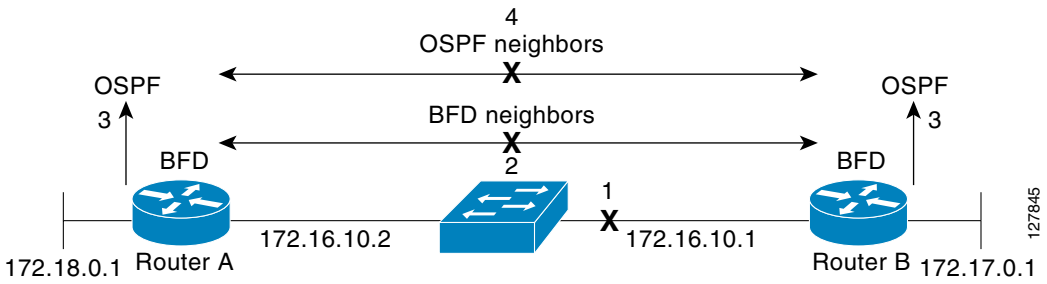


Figure 1-6 shows what happens when a failure occurs in the network (1). The BFD neighbor session with the OSPF neighbor closes (2). BFD notifies the OSPF process that the BFD neighbor is no longer reachable, and the OSPF process breaks the OSPF neighbor relationship (4). When an alternative path is available, the routers start converging on it.

Figure 1-6 Breaking an OSPF Neighbor Relationship



BFD clients are routing protocols that register neighbors with BFD. The switch supports ISIS, OSPF v1 and v2, BGP, EIGRP, and HSRP clients. You can use one BFD session for multiple client protocols. For example, when a network is running OSPF and EIGRP across the same link to the same peer, you need to create only one BFD session, and information is shared with both routing protocols.

The switch supports BFD version 0 and version 1. BFD neighbors automatically negotiate the version and the protocol always runs at the higher version. The default version is version 1.

By default, BFD neighbors exchange both control packets and echo packets for detecting forwarding failures. The switch sends echo packets at the configured BFD interval rate (from 50 to 999 ms on ports or from 600 to999 ms on switch virtual interfaces), and control packets at the BFD slow-timer rate (from 1000 to 3000 ms).

Failure-rate detection can be faster in BFD echo mode, which is enabled by default when you configure BFD session. In this mode, the switch sends echo packets from the BFD software layer, and the BFD neighbor responds to the echo packets through its fast-switching layer. The echo packets do not reach

the BFD neighbor software layer, but are reflected back over the forwarding path for failure detection. You configure the rate at which each BFD interface sends BFD echo packets by entering the **bfd interval** interface configuration command.

To reduce bandwidth consumption, you can disable the sending of echo packets by entering the **no bfd echo** interface configuration command (refer to the section Disabling BFD Echo Mode, page 33). When BFD echo is disabled at one end of a link, the other end of the link also does not send echo packets and does not reflect back the echo packet. Control packets are used to detect forwarding failures. When BFD echo is disabled, the BFD slow-timer configuration does not apply. In a BFD session running in asynchronous mode, BFD packets are exchanged at a negotiated duration when the session is up and at the BFD slow-timer value when the session is down.

To run BFD on a switch, you need to configure basic BFD interval parameters on BFD interfaces, enable routing on the switch, and enable one or more one routing protocol clients for BFD. You also need to confirm that Cisco Express Forwarding (CEF) is enabled (the default) on participating switches.

For more detailed configuration, see the Bidirectional Forwarding Detection feature module at this URL:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fs_bfd.html

For details on the commands, use the Master Index to the Cisco IOS Command List for Release 12.4. at this URL:

http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html

These sections describe how to configure BFD:

Default BFD Configuration

The default BFD settings are as follows:

- No BFD sessions are configured. BFD is disabled on all interfaces.
- When configured, BFD version 1 is the default, but switches negotiate for version. Version 0 is also supported.
- Standby BFD (for HSRP) is enabled by default.
- Asynchronous BFD echo mode is enabled when a BFD session is configured.

BFD Configuration Guidelines

The BFD configuration guidelines are as follows:

- To run BFD on a switch:
  - Configure basic BFD interval parameters on each interface over which you want to run BFD sessions.
  - Enable routing on the switch. You can configure BFD without enabling routing, but BFD sessions do not become active unless routing is enabled on the switch and on the BFD interfaces.

  - Enable one or more one routing protocol clients for BFD. You should implement fast convergence for the routing protocol that you are using. See the IP routing documentation in this chapter or in the *Cisco IOS IP Configuration Guide, Release 12.2,* for information on configuring fast convergence.

Note Cisco recommends that you configure the BFD interval parameters on an interface before configuring the routing protocol commands, especially when using EIGRP.

- Confirm that CEF is enabled on participating switches (the default) as well as IP routing.
- BFD is supported on physical interfaces that are configured as routing interfaces. Starting with Cisco IOS release 12.2(55)SE, BFD is also supported on SVIs. As with physical interfaces, BFD sessions do not operate on an SVI until you put the SVI into Layer 3 mode by assigning it an IP address and enable routing on the switch.

Note Entering the **bfd all-interfaces global configuration command** to enable BFD on all interfaces associated with a routing protocol enables BFD on all physical interfaces and SVIs associated with that routing protocol.

- The switch supports up to 28 BFD sessions at one time.
  - On BFD-enabled ports, the switch supports a minimum hello interval of 50 ms with a multiplier of 3. The multiplier specifies the minimum number of consecutive packets that can be missed before a session is declared down.
  - On BFD-enabled SVI, the minimum hello interval is 600 ms with a multiplier of 3 or higher.
- BFD is not supported on Layer 2 interfaces, pseudowires, static routes, or port channels.
- Although you can configure BFD interface commands on a Layer 2 port, BFD sessions do not operate on the interface unless it is configured as a Layer 3 interface (no switchport) and assigned an IP address.
- In HSRP BFD, standby BFD is enabled globally by default and on all interfaces. When you disable it on an interface, you then must disable and reenable it globally for BFD sessions to be active.
- When using BFD echo mode (the default), you should disable sending of ICMP redirect messages by entering the **no ip redirects** interface configuration command on the BFD interface.

Configuring BFD Session Parameters on an Interface

Before you can start a BFD session on an interface, you must put the interface into Layer 3 mode and set the baseline BFD parameters on it.

Note Although you can configure BFD on Layer 2 interfaces, a BFD session cannot start until both interfaces are in Layer 3 mode and routing is enabled on the switch.

Follow these steps in privileged EXEC mode to configure BFD parameters on any interface participating in a BFD session:

	Command	Description
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface**-*id*	Specifies an interface for a BFD session, and enter interface configuration mode. Physical interfaces and SVIs support BFD.
Step 3	**no shutdown**	Enables the interface if necessary. User network interfaces (UNIs) and enhanced network interfaces (ENIs) are disabled by default; network node interfaces (NNIs) are enabled by default.
Step 4	**no switchport**	Removes the interface from Layer 2 configuration mode (physical interfaces only).
Step 5	**ip address** *ip-address subnet-mask*	Configures the IP address and IP subnet mask.
Step 6	**bfd interval** *milliseconds* **minaret** *milliseconds* **multiplier** *value*	Sets BFD parameters for echo packets on the interface. • **interval**—Specifies the rate at which BFD echo packets are sent to BFD peers. The range is from 50 to 999 milliseconds (ms) on physical interfaces and from 600 to 999 ms on SVIs. • **minaret**—Specifies the rate at which BFD echo packets are expected to be received from BFD peers. The range is from 50 to 999 ms on physical interfaces and from 600 to 999 ms on SVIs. • **multiplier**—Specifies the number of consecutive BFD echo packets that must be missed from a BFD peer before BFD declares that it is unavailable and informs the other BFD peer of the failure. The range is from 3 to 50. **Note** There are no baseline BFD parameter defaults.
Step 7	**end**	Returns to privileged EXEC mode.
Step 8	**show running-config**	Verifies your entries.
Step 9	**show bfd neighbor detail**	(Optional) Displays the final configured or negotiated values when the session is created with a neighbor.
Step 10	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

To remove the BFD parameter configuration, enter the **no bfd interval** interface configuration command.

Enabling BFD Routing Protocol Clients

After you configure BFD parameters on an interface, you can start a BFD session for one or more routing protocols. You must first enable routing by entering the **ip routing** global configuration command on the switch. Note that there can be more than one way to start a BFD session on an interface, depending on the routing protocol.

- Configuring BFD for OSPF, page 29
- Configuring BFD for IS-IS, page 30
- Configuring BFD for BGP, page 32

Configuring BFD for OSPF

When you start BFD sessions for OSPF, OSPF must be running on all participating devices.You can enable BFD support for OSPF by enabling it globally on all OSPF interfaces or by enabling it on one or more interfaces.

Configuring BFD for OSPF Globally

Follow these steps in privileged EXEC mode to configure OSFP BFD globally, and to optionally disable it on specific interfaces:

	Command	Description
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**router ospf** *process- id*	Specifies an OSPF process, and enter router configuration mode.
Step 3	**bfd all-interfaces**	Enables BFD globally on all interfaces associated with the OSPF routing process.
Step 4	**exit**	(Optional) Returns to global configuration mode if you want to disable BFD on one or more OSPF interfaces.
Step 5	**interface** *interface-id*	(Optional) Specifies an interface, and enter interface configuration mode.
Step 6	**ip ospf bfd disable**	(Optional) Disables BFD on the specified OSPF interface. Repeat Steps 5 and 6 for all OSPF interfaces on which you do not want to run BFD sessions.
Step 7	**end**	Returns to privileged EXEC mode.
Step 8	**show bfd neighbors** [**detail**]	Verifies the configuration.
Step 9	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

To disable OSPF BFD on all interfaces, enter the **no bfd all-interfaces** router configuration command.To disable it on an interface, enter the **no ip osfp bfd** or the **ip ospf bfd disable** interface configuration command on the interface.

When you want to run OSPF BFD on only one or a few interfaces, you can enter the **ip ospf bfd** interface configuration command on those interfaces instead of enabling it globally. See the next procedure.

Note When you try to configure OSPF BFD on a Layer 2 interface, the switch does not recognize the configuration.

This is an example of configuring BFD for OSPF on all OSPF interfaces:

```
Switch(config)# router ospf 109
Switch(config-router)# bfd all-interfaces
Switch(config-router)# exit
```

Configuring BFD for OSPF on an Interface

Follow these steps in privileged EXEC mode to configure OSFP BFD on an individual interface:

	Command	Description
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**router ospf** *process- id*	Specifies an OSPF process, and enter router configuration mode.
Step 3	**exit**	Returns to global configuration mode.
Step 4	**interface** *interface-id*	Specifies an interface, and enter interface configuration mode.
Step 5	**ip ospf bfd**	Enables BFD on the specified OSPF interface. Repeat Steps 3 and 4 for all OSPF interfaces on which you want to run BFD sessions.
Step 6	**end**	Returns to privileged EXEC mode.
Step 7	**show bfd neighbors** [**detail**]	Verifies the configuration.
Step 8	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

To disable OSPF BFD on an interface, enter the **no ip osfp bfd** or the **ip ospf bfd disable** interface configuration command on the interface.

This is an example of configuring BFD for OSPF on a single interface:

```
Switch(config)# router ospf 109
Switch(config-router)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip ospf bfd
```

Configuring BFD for IS-IS

When you start BFD sessions for IS-IS, IS-IS must be running on all devices participating in BFD. You can enable BFD support for IS-IS by enabling it globally on all IS-IS interfaces or by enabling it on one or more interfaces.

Configuring BFD for IS-IS Globally

Follow these steps in privileged EXEC mode to configure IS-IS BFD globally, and to optionally disable it on specific interfaces:

	Command	Description
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**router is-is** *area-tag*	Specifies an IS-IS process and enter router configuration mode.
Step 3	**bfd all-interfaces**	Enables BFD globally on all interfaces associated with the IS-IS routing process.
Step 4	**exit**	(Optional) Returns to global configuration mode if you want to disable BFD on one or more IS-IS interfaces.
Step 5	**interface** *interface-id*	(Optional) Specifies an interface and enter interface configuration mode.
Step 6	**ip router isis**	(Optional) Enables IPv4 IS-IS routing on the interface.
Step 7	**isis bfd disable**	(Optional) Disables BFD on the IS-IS interface. Repeat Steps 5 through 7 for all IS-IS interfaces on which you do not want to run BFD sessions.

	Command	Description
Step 8	**end**	Returns to privileged EXEC mode.
Step 9	**show bfd neighbors** [**detail**]	Verifies the configuration.
Step 10	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

To disable IS-IS BFD on all interfaces, enter the **no bfd all-interfaces** router configuration command. To disable it on the specified interface, enter the **no isis bfd** or the **isis bfd disable** interface configuration command on the interface.

When you want to run IS-IS BFD on only a few interfaces, instead of enabling it globally, you can enter the **isis bfd** interface configuration command on those interfaces. See the next procedure.

Note Although IS-IS BFD operates only on Layer 3 interfaces, you can configure it on interfaces in Layer 2 or Layer 3 mode. When you enable it, you see this message:

```
%ISIS BFD is reverting to router mode configuration, and remains disabled.
```

This is an example of setting fast convergence and configuring BFD for IS-IS on all IS-IS interfaces:

```
Switch(config)# router is-is tag1
Switch(config-router)# bfd all-interfaces
Switch(config-router)# exit
```

Configuring BFD for IS-IS on an Interface

Follow these steps in privileged EXEC mode to configure IS-IS BFD on an individual interface:

	Command	Description
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**router is-is** *area-tag*	Specifies an IS-IS process and enter router configuration mode.
Step 3	**exit**	Returns to global configuration mode.
Step 4	**interface** *interface-id*	Specifies an interface, and enter interface configuration mode.
Step 5	**isis bfd**	Enables BFD on the specified IS-IS interface. Repeat Steps 3 and 4 for all IS-IS interfaces on which you want to run BFD sessions.
Step 6	**end**	Returns to privileged EXEC mode.
Step 7	**show bfd neighbors** [**detail**]	Verifies the configuration.
Step 8	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

To disable IS-IS BFD on an interface, enter the **no isis bfd** or the **isis bfd disable** interface configuration command on the interface.

This is an example of configuring BFD for IS-IS on a single interface:

```
Switch(config)# router is-is tag1
Switch(config-router)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# isis bfd
```

Configuring BFD for BGP

When you start BFD sessions for BGP, BGP must be running on all participating devices. You enter the IP address of the BFD neighbor to enable BFD for BGP.

Follow these steps (in privilege EXEC mode) to enable BGP BFD:

	Command	Description
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**router bgp** *as-tag*	Specifies a BGP autonomous system, and enter router configuration mode.
Step 3	**neighbor** *ip-address* **fall-over bfd**	Enables BFD support for fallover on the BFD neighbor.
Step 4	**end**	Returns to privileged EXEC mode.
Step 5	**show bfd neighbors** [**detail**] > **show ip bgp neighbor**	Verifies the configuration. Displays information about BGP connections to neighbors.
Step 6	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

To disable BGP BFD, enter the **no neighbor** *ip-address* **fall-over bfd** router configuration command.

Configuring BFD for EIGRP

When you start BFD sessions for EIGRP, EIGRP must be running on all participating devices.You can enable BFD support for EIGRP by globally enabling it on all EIGRP interfaces or by enabling it on one or more interfaces.

Follow these steps in privileged EXEC mode follow these to configure EIGRP BFD:

	Command	Description
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**router eigrp** *as-number*	Specifies an EIGRP autonomous system number, and enter router configuration mode.
Step 3	**log-adjacency changes** [**detail**]	Configures the switch to send a system logging message when an EIGRP neighbor goes up or down.
Step 4	**bfd {all-interfaces | interface** *interface-id***}**	Enables BFD for EIGRP. • Enters **all-interfaces** to globally enable BFD on all interfaces associated with the EIGRP routing process • Enters **interface** *interface-id* to enable BFD on a per-interface basis for one or more interfaces associated with the EIGRP routing process.
Step 5	**end**	Returns to privileged EXEC mode.
Step 6	**show bfd neighbors** [**detail**]	Verifies the configuration.
Step 7	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

To disable EIGRP BFD on all interfaces, enter the **no bfd all-interfaces** router configuration command. To disable it on an interface, enter the **no bfd interface** *interface-id* router configuration command.

Configuring BFD for HSRP

HSRP supports BFD by default; it is globally enabled on all interfaces. If HSRP support is manually disabled, you can reenable it in interface or global configuration mode. All participating devices must have HSRP enabled and CEF enabled (the default).

Follow these steps in privileged EXEC mode to reenable HSRP BFD:

	Command	Description
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface** *interface-id*	Specifies an interface for a BFD session, and enter interface configuration mode. Only physical interfaces support BFD.
Step 3	**ip address** *ip-address subnet-mask*	Configures the IP address and IP subnet mask for the interface.
Step 4	**standby** [*group-number*] **ip** [*ip-address*] [**secondary**]]	Activates HSRP.
Step 5	**standby bfd**	(Optional) Enables HSRP support for BFD on the interface.
Step 6	**exit**	Returns to global configuration mode.
Step 7	**standby bfd all-interfaces**	(Optional) Enables HSRP support for BFD on all interfaces.
Step 8	**end**	Returns to privileged EXEC mode.
Step 9	**show standby neighbors**	Verifies your entries.
Step 10	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

To disable HSRP support for BFD on all interfaces, enter the **no standby bfd all-interfaces** global configuration command. To disable it on an interface, enter the **no standby bfd** interface configuration command.

Note When you disable standby BFD on an interface by entering the **no standby bfd** interface configuration command and you want to activate BFD sessions on other interfaces, you must globally disable and then reenable standby BFD. Enter the **no standby bfd all-interfaces** global configuration command followed by the **standby bfd all-interfaces** global configuration command.

Disabling BFD Echo Mode

When you configure a BFD session, BFD echo mode is enabled by default on BFD interfaces. You can disable echo mode on an interface. When BFD echo is disabled at one end of a link, the other end of the link also does not send echo packets and does not reflect back the echo packet. Control packets are used to detect forwarding failures. When BFD echo is disabled, the BFD slow-timer configuration does not apply. In a BFD session running in asynchronous mode, BFD packets are exchanged at a negotiated duration when the session is up and at the BFD slow-timer value when the session is down.

Follow these steps in privileged EXEC mode to disable echo mode on a BFD interface:

	Command	Description
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface** *interface-id*	Enters a BFD interface and enter interface configuration mode.

	Command	Description
Step 3	**no bfd echo**	Disables BFD echo mode on the interface. It is enabled by default, but can be disabled independently on BFD neighbors.
Step 4	**exit**	Returns to global configuration mode.
Step 5	**end**	Returns to privileged EXEC mode.
Step 6	**show bfd neighbors detail**	Verifies your entries.
Step 7	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

To reenable echo mode on the interface, enter the **bfd echo** interface configuration command. To reenable echo mode on the switch, enter the **bfd echo** global configuration command.

Related Documents

- Cisco CGS 2520 Software Configuration Guides:

  http://www.cisco.com/en/US/products/ps10978/products_installation_and_configuration_guides_list.html

- Cisco CGS 2520 Release Notes:

  http://www.cisco.com/en/US/products/ps10978/prod_release_notes_list.html

Technical Assistance

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml