CHAPTER 53

Configuring Ethernet CFM and OAM

Ethernet Operations, Administration, and Maintenance (OAM) is a protocol for installing, monitoring, and troubleshooting Ethernet networks to enhance management within the Ethernet infrastructure. The Catalyst 4500 series switch supports IEEE 802.1ag Connectivity Fault Management (CFM) and IEEE 802.3ah Ethernet OAM discovery, link monitoring, remote fault detection, and remote loopback. The Ethernet OAM manager controls the interaction between CFM and OAM.

For complete command and configuration information for CFM, see the Cisco IOS feature module at this URL:

http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_cfm.html

This chapter contains these sections:

Command List

This table lists the commands most commonly used with Ethernet CFM and OAM.

Command	Purpose	Location
`Switch(config-if)# no ehernet cfm enable`	Disables CFM globally.	Disabling CFM on a Port, page 53-9
`Switch(config)# ethernet cfm traceroute cache [size entries | hold-time minutes]`	(Optional) Configures the CFM traceroute cache.	Configuring the Ethernet CFM Service over VLANs, page 53-10

Command	Purpose	Location
`Switch(config)# ethernet cfm domain domain-name level level-id {direction outward}`	Defines a CFM domain, sets the domain level, and enters ethernet-cfm configuration mode for the domain.	Configuring the Ethernet CFM Service over VLANs, page 53-10
`Switch(config-ether-cfm)# [no] service csi-id vlan vlan-id`	Sets a universally unique ID for the customer within a maintenance domain for an EVC.	Configuring the Ethernet CFM Service over VLANs, page 53-10
`Switch(config-ether-cfm)# mep archive-hold-time minutes`	(Optional) Sets the number of minutes that data from a missing maintenance end point (mep) is kept before it is purged.	Configuring the Ethernet CFM Service over VLANs, page 53-10
`Switch(config-if)# ethernet cfm mip level level-id`	Configures an operator-level maintenance intermediate point (MIP) for a domain level-ID	Configuring the Ethernet CFM Service over VLANs, page 53-10
`Switch(config-if)# ethernet cfm mep level level-id {[inward] | outward} mpid id vlan {vlan-id | any | vlan-id-vlan-id [,vlan-id-vlan-id]}`	(Optional) Configures maintenance end points (MEPs). for different maintenance levels.	Configuring the Ethernet CFM Service over VLANs, page 53-10
`Switch(config)# ethernet cfm cc {[enable] level {level-id | any} vlan {vlan-id | any}}`	Configures per domain continuity check (cc) parameters. The level ID identifies the domain to which configuration applies.	Configuring the Ethernet CFM Service over VLANs, page 53-10
`Switch(config)# snmp-server enable traps ethernet cfm cc [mep-up] [mep-down] [config] [loop] [cross-connect]`	(Optional) Enables Ethernet CFM continuity check traps.	Configuring the Ethernet CFM Service over VLANs, page 53-10
`Switch(config)# snmp-server enable traps ethernet cfm crosscheck [mep-unknown] [mep-missing] [service-up]`	(Optional) Enables Ethernet CFM crosscheck traps.	Configuring the Ethernet CFM Service over VLANs, page 53-10

Ethernet CFM Overview

Ethernet CFM is an end-to-end per-service-instance (per VLAN) Ethernet layer OAM protocol. It includes proactive connectivity monitoring, fault verification, and fault isolation. End-to-end can be provider-edge-to provider-edge (PE-to-PE) device or customer-edge-to-customer-edge (CE-to-CE) device. Ethernet CFM, as specified by IEEE 802.1ag, is the standard for Layer 2 ping, Layer 2 traceroute, and end-to-end connectivity verification of the Ethernet network.

Unlike CFM, other metro-Ethernet OAM protocols are not end-to-end technologies. For example, IEEE 802.3ah OAM is a single-hop and per-physical-wire protocol and is not end-to-end or service aware.

These sections contain conceptual information about Ethernet CFM:

- Definition List, page 53-3
- CFM Domain, page 53-3
- CFM Maintenance Points, page 53-4
- General Packet Forwarding Rules, page 53-5

Definition List

Term	Definition
CC	Ethernet OAM Continuity Check
CFM	Ethernet Connectivity Fault Management
EI	Ethernet Infrastructure or EVC Infrastructure
EVC	Ethernet Virtual Circuit
MEP	Maintenance Endpoint
MIP	Maintenance Intermediate Point
OAM	Operations Administration and Maintenance
UNI	User to Network Interface

CFM Domain

A CFM maintenance domain is a management space on a network that is owned and operated by a single entity and defined by a set of internal boundary ports. You assign a unique maintenance level (from 0 to 7) to define the domain hierarchy. The larger the domain, the higher the level. For example, as shown in Figure 53-1, a service-provider domain would be larger than an operator domain and might have a maintenance level of 6, while the operator domain maintenance level would be 3 or 4.

As shown in Figure 53-2, domains cannot intersect or overlap because that would require management by more than one entity, which is not allowed. Domains can touch or nest (if the outer domain has a higher maintenance level than the nested domain). Nesting domains can be useful when a service provider contracts with one or more operators to provide Ethernet service. Each operator has its own maintenance domain and the service provider domain is a superset of the operator domains. Maintenance levels of nesting domains should be communicated among the administrating organizations. CFM exchanges messages and performs operations on domains individually.

Figure 53-1 CFM Maintenance Domains

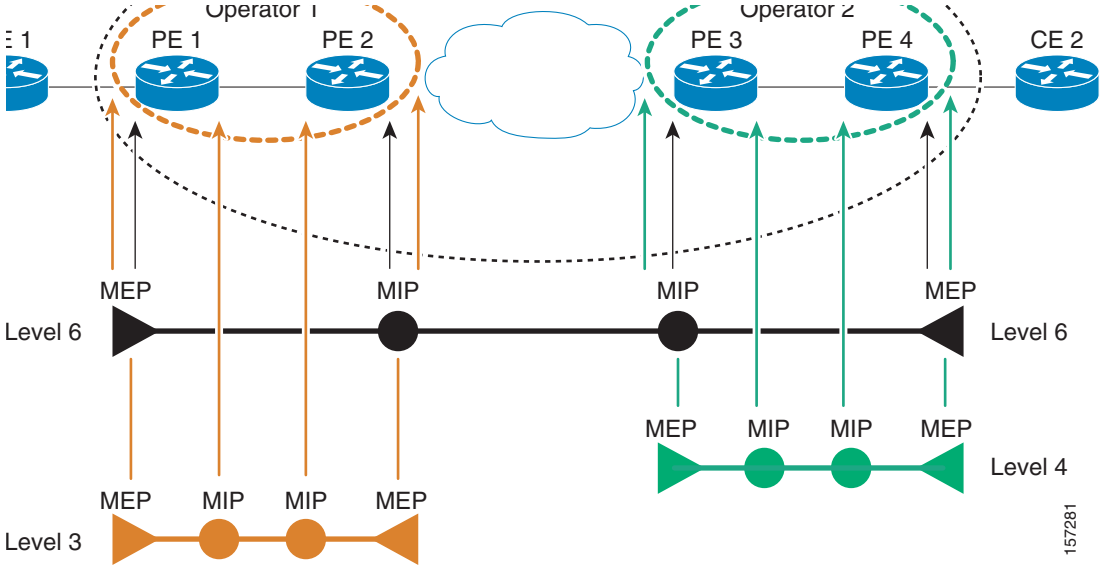
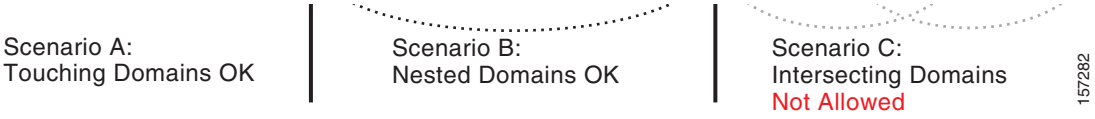


Figure 53-2 Allowed Domain Relationships



CFM Maintenance Points

Operating with a maintenance domain, a maintenance point demarcates an interface that participates in an CFM. Maintenance points drop all lower-level frames and forward all higher-level frames. There are two types of maintenance points:

- Maintenance end points (MEPs) are points at the edge of the domain that define the boundary and confine CFM messages within the boundary. *MEPs are inward facing by default. Inward facing* means that they communicate through the relay function side, not the wire side (connected to the port), whereas MEPs that can be configured as outward facing communicate through the wire side, and not through the relay function side.

  An *inward-facing* MEP sends and receives CFM frames through the relay function. It drops all CFM frames at its level or lower that come from the wire side. For CFM frames from the relay side, it processes the frames at its level and drops frames at a lower level. The MEP

transparently forwards all CFM frames at a higher level, whether they are received from the relay or wire side. CFM runs at the provider maintenance level (UPE-to-UPE), specifically with inward-facing MEPs at the user network interface (UNI).

An *outward facing* MEP (OFM) sends and receives CFM frames on the wire side. It drops all CFM frames at its level or lower that come from the relay function side. For CFM frames from the wire side, it processes the frames at its level and drops frames at a lower level. OFM transparently forwards all CFM frames at a higher level, whether they are received from the relay or wire side.

- Maintenance intermediate points (MIPs) are inside a domain, not at the boundary, and respond to CFM only when triggered by traceroute and loopback messages. They forward CFM frames received from MEPs and other MIPs, drop all CFM frames at a lower level, and forward all CFM frames at a higher level, whether they are received from the relay or wire side.

If a port on which the inward facing MEP is configured is blocked by Spanning-Tree Protocol (STP), the MEP cannot receive or transmit CFM messages. If a port on which the outward facing MEP is configured is blocked by STP, the OFM can only receive CFM messages from and transmit them towards the wire. If a port on which a MIP is configured is blocked by STP, the port cannot receive or respond to messages from the relay function side, but can receive CFM messages and respond to them from the wire side.

General Packet Forwarding Rules

Ethernet CFM frames should be forwarded or dropped based on the strict rules of hierarchical maintenance domains. MEPs and MIPs configured on bridge ports act as filters that confine CFM frames within the bounds of the correct domain(s) by dropping frames that do not belong to the correct Level.

Topics include:

Inward-Facing MEPs

An inward-facing MEP does the following:

- Sends and receives CFM frames at its level through the relay function, not through the wire connected to the port on which the MEP is configured.
- Drops all CFM frames at its level (or lower level) that come from the wire side.
- Processes all CFM frames at its level that come from the direction of the relay function.

  A packet arriving on a wire at a port is coming from the wire side.

  A packet arriving internally from the CPU or by the bridging action in hardware (or software) is coming from the relay function side.
- Drops all CFM frames at a lower level that come from the direction of the relay function.
- Transparently forwards all CFM frames at a higher level, whether they come from the relay function or the wire side.

Note A MEP of level L (where L != 7) requires a MIP of level M > L on the same port. So, CFM frames at a higher level than the MEP are cataloged by this MIP.

- If the port on which the MEP is configured is blocked by STP, the MEP can no longer transmit or receive CFM messages.

Note On Catalyst 4500 Supervisor Engine 6-ME, outward MEPs are only supported on the supervisor uplink ports.

Outward-Facing MEPs

An outward-facing MEP does the following:

- Sends and receives CFM frames at its level through the wire connected to the port through which the MEP is configured.
- Drops all CFM frames at its level (or lower level) that come from the relay function side.
- Processes all CFM frames at its level coming from the direction of the wire.
- Drops all CFM frames at a lower level coming from the direction of the wire.
- Transparently forwards all CFM frames at a higher level, whether they come in from the relay function side or the wire side.

  A MEP of level L (where L != 7) requires a MIP of level M > L on the same port. So, CFM frames at a higher level than the MEP are catalogued by this MIP.
- If the port on which the MEP is configured is blocked by STP, the MEP can still transmit and receive CFM messages through the wire.
- A MIP catalogues and forwards CFM frames at its level both through the wire and through the relay function.
- A MIP stops and drops all CFM frames at a lower level whether they come from the wire or relay function side.
- A MIP transparently forwards CFM frames at a higher level whether they come from the wire or relay function side.
- If the port on which the MIP is configured is blocked by STP, the MIP cab no longer receive or relay CFM messages towards the relay function side; however, it can still receive and respond to CFM messages from the wire.

Transparent Ports

A transparent port has neither a MEP nor MIP configured, and forwards CFM frames like regular data traffic.

STP blocking applies to CFM frames on transparent ports just as it applies to ports with inward-facing MEPs; if the port is blocked by STP, CFM frames are dropped as they attempt to ingress or egress that port.

CFM Messages

CFM uses standard Ethernet frames distinguished by EtherType or (for multicast messages) by MAC address. All CFM messages are confined to a maintenance domain and to a service-provider VLAN (S-VLAN). Four CFM messages are supported:

- **Continuity Check (CC) messages**—multicast heartbeat messages exchanged periodically between MEPs that allow MEPs to discover other MEPs within a domain and allow MIPs to discover MEPs. CC messages are confined to a domain or VLAN.
- **Loopback messages**—unicast frames transmitted by a MEP at administrator request to verify connectivity to a particular maintenance point, indicating whether a destination is reachable. A loopback message is similar to an Internet Control Message Protocol (ICMP) ping message.
- **Traceroute messages**—multicast frames transmitted by a MEP at administrator request to track the path (hop-by-hop) to a destination MEP. Traceroute messages are similar in concept to UDP traceroute messages.
- **AIS messages**—described in Chapter 53, "Configuring Ethernet CFM and OAM."

Crosscheck Function

The crosscheck function verifies a post-provisioning timer-driven service between dynamically configured MEPs (using crosscheck messages) and expected MEPs (by configuration) for a service. It verifies that all endpoints of a multipoint service are operational. The crosscheck function is performed only one time and is initiated from the command-line interface (CLI).

SNMP Traps

The MEPs generate two types of SMNP traps: CC traps and crosscheck traps.

Supported CC traps include:

- MEP up
- MEP down
- cross-connect (a service ID does not match the VLAN)
- loop
- configuration error

Supported crosscheck traps include:

- service up
- MEP missing (an expected MEP is down)
- unknown MEP

IP SLAs Support for CFM

The Metro switch supports CFM with IP Service Level Agreements (SLAs), which gathers Ethernet layer network performance metrics. Available statistical measurements for the IP SLAs CFM operation include round-trip time, jitter (interpacket delay variance), and packet loss. You can schedule multiple IP SLA operations and use Simple Network Management Protocol (SNMP) trap notifications and syslog messages to monitor threshold violations proactively.

IP SLA integration with CFM gathers Ethernet layer statistical measurements by sending and receiving Ethernet data frames between CFM MEPs. Performance is measured between the source MEP and the destination MEP. Unlike other IP SLA operations that provide performance metrics for only the IP layer, IP SLAs with CFM provide performance metrics for Layer 2.

You can manually configure individual Ethernet ping or jitter operations. You can also configure an IP SLA automatic Ethernet operation that queries the CFM database for all MEPs in a given maintenance domain and VLAN. The operation then automatically creates individual Ethernet ping or jitter operations based on the discovered MEPs.

For more information about IP SLA operation with CFM, see the *IP SLAs for Metro-Ethernet* feature module at this URL:

http://www.cisco.com/en/US/docs/ios/12_2sr/12_2srb/feature/guide/sr_meth.html

Configuring Ethernet CFM

To configure Ethernet CFM you must prepare the network and configuring services. You can optionally configure and enable crosschecking. These sections are included:

Default Ethernet CFM Configuration

CFM is globally disabled.

CFM is enabled on all interfaces. A port can be configured as a flow point (MIP/MEP), a transparent port, or disabled (CFM disabled). By default, ports are transparent until configured as MEP, MIP, or disabled.

There are no MEPs or MIPs configured.

Ethernet CFM Configuration Guidelines

These are the configuration guidelines and restrictions for CFM:

- A MIP should be configured on a port before a MEP, unless the MEP is at level 7 or the MEP is an outward-facing MEP (OFM). Similarly, all the MEPs have to be removed before a MIP on a port.
- CFM Unicast packets (Loopback Messages and Traceroute Reply), are not allowed on an OFM on STP blocked ports. So, the blocked port cannot respond to ping and traceroute.
- CFM is not supported and cannot be configured on routed ports.
- CFM is not supported and cannot be configured on dot1q-tunnel ports.
- CFM is supported on EtherChannel port channels. You can configure an EtherChannel port channel as MEP or MIP. However, CFM is not supported on individual ports that belong to an EtherChannel and you cannot add a CFM port to an EtherChannel group.
- You cannot configure CFM on VLAN interfaces.

- You cannot configure CFM on an EoMPLS port.
- CFM is not supported and cannot be configured on a PVLAN isolated host port, community host port or promiscuous access port.
- CFM is supported only on regular VLANs for inward-facing MEP on PVLAN trunks. Whereas OFM is supported on regular VLANs and isolated VLANs on PVLAN secondary trunk, similarly OFM is supported on regular VLANs and primary VLANs on promiscuous trunk ports.

  The CFM service on a PVLAN ends at the PVLAN trunk. The translation of CFM service from one PVLAN to another PVLAN is not supported between the PVLAN trunks.

Disabling CFM on a Port

When CFM is globally enabled, you might want to disable CFM selectively on a port (or port channel).

Note By default, CFM is globally disabled and enabled at every port.

To configure the network for Ethernet CFM over VLANs, follow these steps:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# interface interface-id`	Specify a physical interface or a port channel to configure, and enter interface configuration mode.
Step 3	`Switch(config-if)# no ethernet cfm enable`	Disables CFM globally. When CFM is disabled on an interface, all CFM frames that arrive at that interface are forwarded as normal data traffic, and are not processed by the CPU.
Step 4	`Switch(config-if)# exit`	Returns to global configuration mode.
Step 5	`Switch(config)# end`	Return to privileged EXEC mode.

Configuring the Ethernet CFM Service over VLANs

To configure the network for Ethernet CFM over VLANs, follow these steps:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# ethernet cfm enable`	Enables CFM globally.
Step 3	`Switch(config)# vlan vlan-id`	Specifies the VLAN.

	Command	Purpose
Step 4	`Switch(config)# ethernet cfm traceroute cache [size entries | hold-time minutes]`	(Optional) Configures the CFM traceroute cache. You can set a maximum cache size or hold time. • (Optional) For **size**, enter the cache size in number of entry lines. The range is from 1 to 4095; the default is 100 lines. • (Optional) For **hold-time**, enter the maximum cache hold time in minutes. The range is from 1 to 65535; the default is 100 minutes.
Step 5	`Switch(config)# ethernet cfm domain domain-name level level-id {direction outward}`	Defines a CFM domain, sets the domain level, and enters ethernet-cfm configuration mode for the domain. The maintenance level number range is 0 to 7. Configures direction as outward, which is required to configure OFM.
Step 6	`Switch(config-ether-cfm)# [no] service csi-id vlan vlan-id`	Sets a universally unique ID for the customer within a maintenance domain for an EVC.
Step 7	`Switch(config-ether-cfm)# mep archive-hold-time minutes`	(Optional) Sets the number of minutes that data from a missing maintenance end point (mep) is kept before it is purged. The range is 1 to 65535; the default is 100 minutes.
Step 8	`Switch(config-ether-cfm)# exit`	Returns to global configuration mode.
Step 9	`Switch(config)# interface interface-id`	Specifies a physical interface or a port channel to configure, and enter interface configuration mode.
Step 10	`Switch(config-if)# ethernet cfm mip level level-id`	Configures an operator-level maintenance intermediate point (MIP) for the domain level-ID defined in Step 3. **Note** If you plan to configure a MEP at level 7 on this interface, do not use this command to configure a MIP on the interface.
Step 11	`Switch(config-if)# ethernet cfm mep level level-id {[inward] | outward} mpid id vlan {vlan-id | any | vlan-id-vlan-id [,vlan-id-vlan-id]}`	(Optional) Configures maintenance end points (MEPs). for different maintenance levels. The MEP level range is 0 to 7. • Specify the direction for the end point (Required for Outward, Optional for inward direction). • For **mpid** *identifier*, enter a maintenance end point identifier. The identifier must be unique for each VLAN (service instance). The range is 1 to 8191. • For **vlan** *vlan-id*, enter the service provider VLAN ID or IDs as a VLAN-ID (1 to 4095), a range of VLAN-IDs separated by a hyphen, or a series of VLAN IDs separated by comma. **Note** Repeat the command for different level IDs.
Step 12	`Switch(config-ether-cfm)# exit`	Returns to global configuration mode.

	Command	Purpose
Step 13	`Switch(config)# ethernet cfm cc {[enable] level {level-id | any} vlan {vlan-id | any}}`	Configures per domain continuity check (cc) parameters. The level ID identifies the domain to which configuration applies. • Enter **enable** to enable CFM cc for the domain level. • Enter a maintenance **level** as a level number (0 to 7) or as **any** for all maintenance levels. • Enter the VLANs to apply the check to, as a VLAN-ID (1 to 4095), a range of VLAN-IDs separated by a hyphen, a series of VLAN IDs separated by commas, or **any** for any VLANs.
Step 14	`Switch(config)# snmp-server enable traps ethernet cfm cc [mep-up] [mep-down] [config] [loop] [cross-connect]`	(Optional) Enables Ethernet CFM continuity check traps.
Step 15	`Switch(config)# snmp-server enable traps ethernet cfm crosscheck [mep-unknown] [mep-missing] [service-up]`	(Optional) Enables Ethernet CFM crosscheck traps.
Step 16	`Switch(config)# end`	Returns to privileged EXEC mode.

Step 17	`Switch# show ethernet cfm domain brief`
	`Switch# show ethernet cfm maintenance-points local`
	`Switch# show ethernet cfm traceroute-cache`
		Verifies the configuration.

Step 18	`Switch# show running-config`	Verifies your entries.
Step 19	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Use the **no** versions of the commands to remove the configuration or return to the default configurations.

Configuring Ethernet CFM Crosscheck for VLANs

To configure Ethernet CFM crosscheck for VLANs, follow these steps:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# ethernet cfm mep crosscheck start-delay delay`	Configures the number of seconds that the device waits for remote MEPs to come up before the crosscheck is started. The range is 1 to 65535; the default is 30 seconds.
Step 3	`Switch(config)# ethernet cfm domain domain-name level level-id {direction outward}`	Defines a CFM domain, set the domain level, and enter ethernet-cfm configuration mode for the domain. The maintenance level number range is 0 to 7. Configure direction as outward, which is required to configure OFM.

	Command	Purpose
Step 4	`Switch(config-ether-cfm)# mep crosscheck mpid` *identifier* `vlan` *vlan-id* `[mac` *remote MAC address*`]`	Defines a remote maintenance end point (MEP) within a maintenance domain. • For **mpid** *identifier*, enter the remote MEP's maintenance end point identifier. The range is 1 to 8191. • For **vlan** *vlan-id*, the VLAN range is from 1 to 3581. • (Optional) Specify the MAC address of the remote MEP.
Step 5	`Switch(config)# end`	Returns to privileged EXEC mode.
Step 6	`Switch# ethernet cfm mep crosscheck {enable | disable} level` *level-id* `vlan {`*vlan-id* `| any}`	Enables or disables CFM crosscheck for one or more maintenance levels and VLANs. • For **level** *level-id*, enter a single level ID (0 to 7), a range of level IDs separated by a hyphen, or a series of level IDs separated by commas. • For **vlan** *vlan-id*, enter the provider VLAN ID or IDs as a VLAN-ID (1 to 3581), a range of VLAN-IDs separated by a hyphen, or a series of VLAN IDs separated by commas, or enter **any** for any VLAN.
Step 7	`Switch# show ethernet cfm maintenance-points remote crosscheck`	Verifies the configuration.
Step 8	`Switch# show ethernet cfm errors`	Displays the results of the crosscheck operation.
Step 9	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Use the **no** form of each command to remove a configuration or to return to the default settings.

Configuring IP SLAs CFM Operation

You can manually configure an IP SLA's Ethernet ping or jitter echo operation, or you can configure IP SLAs Ethernet operation with endpoint discovery. You can also configure multiple operation scheduling. For accurate one-way delay statistics, the clocks on the endpoint switches must be synchronized. You can configure the endpoint switches with Network Time Protocol (NTP) so that the switches are synchronized to the same clock source.

Note When you configure the Catalyst 4500 series switch for a class of service (CoS) probe, you must first globally enable QoS by entering the **mls qos** global configuration command.

For detailed information about configuring IP SLAs operations, see the *Cisco IOS IP SLAs Configuration Guide, Release 12.4T* at this URL:

http://www.cisco.com/en/US/products/ps6441/products_installation_and_configuration_guides_list.html

For detailed information about IP SLAs commands, see the command reference at this URL:

http://www.cisco.com/en/US/docs/ios/ipsla/command/reference/sla_book.html

This section includes these procedures:

Manually Configuring an IP SLAs CFM Probe or Jitter Operation

To manually configure an IP SLAs Ethernet echo (ping) or jitter operation, follow these steps:

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**ip sla** *operation-number*	Creates an IP SLAs operation, and enters IP SLAs configuration mode.
Step 3	**ethernet echo mpid** *identifier* **domain** *domain-name* **vlan** *vlan-id* or **ethernet jitter mpid** *identifier* **domain** *domain-name* **vlan** *vlan-id* [**interval** *interpacket-interval*] [**num-frames** *number-of frames transmitted*]	Configures the IP SLAs operation as an echo (ping) or jitter operation, and enter IP SLAs Ethernet echo configuration mode. • Enter **echo** for a ping operation or **jitter** for a jitter operation. • For **mpid** *identifier*, enter a maintenance endpoint identifier. The identifier must be unique for each VLAN (service instance). The range is 1 to 8191. • For **domain** *domain-name*, enter the CFM domain name. • For **vlan** *vlan-id*, the VLAN range is from 1 to 4095. • (Optional—for jitter only) Enter the **interval** between sending of jitter packets. • (Optional—for jitter only) Enter the **num-frames** and the number of frames to be sent.
Step 4	**cos** *cos-value*	(Optional) Sets a class of service value for the operation. Before configuring the **cos** parameter on the Catalyst 3750 Metro switch, you must globally enable QoS by entering the **mls qos** global configuration command.
Step 5	**frequency** *seconds*	(Optional) Sets the rate at which the IP SLAs operation repeats. The range is from 1 to 604800 seconds; the default is 60 seconds.
Step 6	**history** *history-parameter*	(Optional) Specifies parameters for gathering statistical history information for the IP SLAs operation.
Step 7	**owner** *owner-id*	(Optional) Configures the SNMP owner of the IP SLAs operation.
Step 8	**request-data-size** *bytes*	(Optional) Specifies the protocol data size for an IP SLAs request packet. The range is from 0 to the maximum size allowed by the protocol being used; the default is 66 bytes.
Step 9	**tag** *text*	(Optional) Creates user-specified identifier for an IP SLAs operation.

	Command	Purpose
Step 10	**threshold** *milliseconds*	(Optional) Specifies the upper threshold value in milliseconds (ms) for calculating network monitoring statistics. The range is 0 to 2147483647; the default is 5000.
Step 11	**timeout** *milliseconds*	(Optional) Specifies the amount of time in ms that the IP SLAs operation waits for a response from its request packet. The range is 0 to 604800000; the default value is 5000.
Step 12	**exit**	Returns to global configuration mode.
Step 13	**ip sla schedule** *operation-number* [**ageout** *seconds*] [**life** {**forever** | *seconds*}] [**recurring**] [**start-time** {*hh:mm {:ss}* [*month day* | *day month*] | **pending** | **now** | **after** *hh:mm:ss*}]	Schedules the time parameters for the IP SLAs operation. • *operation-number*—Enter the IP SLAs operation number. • (Optional) **ageout** *seconds*—Enter the number of seconds to keep the operation in memory when it is not actively collecting information. The range is 0 to 2073600 seconds. The default is 0 seconds. • (Optional) **life**—Set the operation to run indefinitely (**forever**) or for a specific number of *seconds*. The range is from 0 to 2147483647. The default is 3600 seconds (1 hour) • (Optional) **recurring**—Set the probe to be automatically scheduled every day. • (Optional) **start-time**—Enter the time for the operation to begin collecting information: – To start at a specific time, enter the hour, minute, second (in 24-hour notation), and day of the month. – Enter **pending** to select no information collection until a start time is selected. – Enter **now** to start the operation immediately. – Enter **after** *hh:mm:ss* to show that the operation should start after the entered time has elapsed.
Step 14	**end**	Returns to privileged EXEC mode.
Step 15	**show ip sla configuration** [*operation-number*]	Shows the configured IP SLAs operation.
Step 16	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

To remove an IP SLAs operation, enter the **no ip sla** *operation-number* global configuration command.

Configuring an IP SLAs Operation with Endpoint Discovery

To use IP SLAs to automatically discover the CFM endpoints for a domain and VLAN ID, follow these steps. You can configure ping or jitter operations to the discovered endpoints.

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**ip sla ethernet-monitor** *operation-number*	Begins configuration of an IP SLAs automatic Ethernet operation, and enter IP SLAs Ethernet monitor configuration mode.
Step 3	**type echo domain** *domain-name* **vlan** *vlan-id* [**exclude-mpids** *mp-ids*] or **type jitter domain** *domain-name* **vlan** *vlan-id* [**exclude-mpids** *mp-ids*] [**interval** *interpacket-interval*] [**num-frames** *number-of frames transmitted*]	Configures the automatic Ethernet operation to create echo (ping) or jitter operation and enters IP SLAs Ethernet echo configuration mode. • Enter **type echo** for a ping operation or **type jitter** for a jitter operation. • For **mpid** *identifier*, enter a maintenance endpoint identifier. The range is 1 to 8191. • For **domain** *domain-name*, enter the CFM domain name. • For **vlan** *vlan-id*, the VLAN range is from 1 to 4095. • (Optional) Enter **exclude-mpids** *mp-ids* to exclude the specified maintenance endpoint identifiers. • (Optional—for jitter only) Enter the **interval** between sending of jitter packets. • (Optional—for jitter only) Enter the **num-frames** and the number of frames to be sent.
Step 4	**cos** *cos-value*	(Optional) Sets a class of service value for the operation.
Step 5	**owner** *owner-id*	(Optional) Configures the SNMP owner of the IP SLAs operation.
Step 6	**request-data-size** *bytes*	(Optional) Specifies the protocol data size for an IP SLAs request packet. The range is from 0 to the maximum size allowed by the protocol being used; the default is 66 bytes.
Step 7	**tag** *text*	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 8	**threshold** *milliseconds*	(Optional) Specifies the upper threshold value in milliseconds for calculating network monitoring statistics. The range is 0 to 2147483647; the default is 5000.
Step 9	**timeout** *milliseconds*	(Optional) Specifies the amount of time in milliseconds that the IP SLAs operation waits for a response from its request packet. The range is 0 to 604800000; the default value is 5000.
Step 10	**exit**	Returns to global configuration mode.

	Command	Purpose
Step 11	**ip sla schedule** *operation-number* [**ageout** *seconds*] [**life** {**forever** | *seconds*}] [**recurring**] [**start-time** {*hh:mm {:ss}* [*month day* | *day month*] | **pending** | **now** | **after** *hh:mm:ss*}]	Schedules the time parameters for the IP SLAs operation. • *operation-number*—Enter the IP SLAs operation number. • (Optional) **ageout** *seconds*—Enter the number of seconds to keep the operation in memory when it is not actively collecting information. The range is 0 to 2073600 seconds. The default is 0 seconds. • (Optional) **life**—Set the operation to run indefinitely (**forever**) or for a specific number of *seconds*. The range is from 0 to 2147483647. The default is 3600 seconds (1 hour) • (Optional) **recurring**—Set the probe to be automatically scheduled every day. • (Optional) **start-time**—Enter the time for the operation to begin collecting information: – To start at a specific time, enter the hour, minute, second (in 24-hour notation), and day of the month. – Enter **pending** to select no information collection until a start time is selected. – Enter **now** to start the operation immediately. – Enter **after** *hh:mm:ss* to show that the operation should start after the entered time has elapsed.
Step 12	**end**	Returns to privileged EXEC mode.
Step 13	**show ip sla configuration** [*operation-number*]	Shows the configured IP SLAs operation.
Step 14	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

To remove an IP SLAs operation, enter the **no ip sla** *operation-number* global configuration command.

Example: Switchport/VLAN CFM with an Inward-Facing MEP

The following is an example of a VLAN-based CFM configuration between two switches. In this example, a Supervisor Engine II+10GE switch called *g6-1* is connected to a Metro Ethernet Supervisor Engine 6-E switch called *Switch*. Gi 6/5 of g6-1 is connected to the gi 3/5 of the Switch through an ethernet cable.

Configuration on the Supervisor Engine II+10GE (“g6-1”)

```
-----------------------------------------------------

!
ethernet cfm domain customer2 level 6
ethernet cfm domain PROVIDER2 level 5
 service customerX vlan 102
ethernet cfm enable
!
!
vlan 102
```

```
!
interface GigabitEthernet6/2
 switchport access vlan 102
 ethernet cfm mip level 6
 ethernet cfm mep level 5 mpid 2101 vlan 102
!
interface GigabitEthernet6/5
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 102
 switchport mode trunk
 ethernet cfm mip level 5
!
ethernet cfm cc enable level 5 vlan 102
!
```

Screen dumps from “g6-1”

```
g6-1# show ethernet cfm main rem
Can only Ping/Traceroute to remote MEPs marked with *

--------------------------------------------------------------------------------
MPID Level Mac Address  Vlan PortState InGressPort  Age(sec)    Service ID
--------------------------------------------------------------------------------
2111*  5     001b.d550.90fd  102   UP            Gi6/5                 6
customerX

Total Remote MEPs: 1
g6-1#

g6-1# show ethernet cfm main local
sh ethernet cfm main local
--------------------------------------------------------------------------------
MPID Level Type VLAN Port    CC-Status MAC             DomainName
--------------------------------------------------------------------------------
2101    5      MEP I 102     Gi6/2      Enabled   000a.4172.df3d              PROVIDER2


--------------------------------------------------------------------------------
Level Type  Port                      MAC
--------------------------------------------------------------------------------
6     MIP   Gi6/2                     000a.4172.df3d
5     MIP   Gi6/5                     000a.4172.df3d
g6-1#
```

Configuration on the Metro Ethernet Supervisor Engine 6-E Switch (“Switch”)

```
!
ethernet cfm domain customer2 level 6
ethernet cfm domain PROVIDER2 level 5
 service customerX vlan 102
ethernet cfm enable
!
vlan 102
!
interface GigabitEthernet3/1
 switchport mode trunk
 ethernet cfm mip level 6
 ethernet cfm mep level 5 mpid 2111 vlan 102
!
interface GigabitEthernet3/5
 switchport mode trunk
```

```
 ethernet cfm mip level 5
!
ethernet cfm cc enable level 5 vlan 102
!
```

Screen dumps on “Switch"

```
-----------------------------------------------------

Switch# show ethernet cfm main rem
Can only Ping/Traceroute to remote MEPs marked with *

MPID  Level Mac Address    Vlan PortState InGressPort   Age(sec) Service ID
2101*    5     000a.4172.df3d 102   UP          Gi3/5            1              customerX
Total Remote MEPs: 1
Switch# show ethernet cfm main local
MPID DomainName     Level Type  VLAN   Port       CC-Status    MAC
2111 PROVIDER2         5        MEP 102         Gi3/1   Enabled        001b.d550.90fd

Level Type  Port                      MAC
6     MIP   Gi3/1                     001b.d550.90fd
5     MIP   Gi3/5                     001b.d550.90fd
```

Displaying Ethernet CFM Information

To display Ethernet CFM information, you can use the privileged EXEC commands in Table 53-1.

Table 53-1 Displaying CFM Information

Command	Purpose
show ethernet cfm domain brief	Displays brief details about CFM maintenance domains.
show ethernet cfm errors	Displays CFM continuity check error conditions logged on a device since it was last reset or since the log was last cleared. When CFM crosscheck is enabled, displays the results of the CFM crosscheck operation.
show ethernet cfm maintenance-points local	Displays maintenance points configured on a device.
show ethernet cfm maintenance-points remote [detail | domain | level]	Displays information about a remote maintenance point domains or levels or details in the CFM database.
show ethernet cfm maintenance-points remote crosscheck	Displays information about remote maintenance points configured statically in a crosscheck list.
show ethernet cfm traceroute-cache	Displays the contents of the traceroute cache.

To display IP SLAs Ethernet CFM information, you can use the privileged EXEC commands in Table 53-2.

Table 53-2 Displaying IP SLAs CFM Information

Command	Purpose
show ip sla configuration [*entry-number*]	Displays configuration values including all defaults for all IP SLAs operations or a specific operation.
show ip sla ethernet-monitor configuration [*entry-number*]	Displays the configuration of the IP SLAs automatic Ethernet operation.
show ip sla statistics [*entry-number* | **aggregated** | **details**]	Display current or aggregated operational status and statistics.

Ethernet OAM Protocol Overview

The Ethernet OAM protocol for installing, monitoring, and troubleshooting Metro Ethernet networks and Ethernet WANs relies on an optional sublayer in the data link layer of the OSI model. Normal link operation does not require Ethernet OAM. You can implement Ethernet OAM on any full-duplex point-to-point or emulated point-to-point Ethernet link for a network or part of a network (specified interfaces).

OAM frames, called OAM protocol data units (OAM PDUs) use the slow protocol destination MAC address 0180.c200.0002. They are intercepted by the MAC sublayer and cannot propagate beyond a single hop within an Ethernet network. Ethernet OAM is a relatively slow protocol, with a maximum transmission rate of 10 frames per second, resulting in minor impact to normal operations. However, because the CPU must poll error counters frequently, when you enable link monitoring, the number of required CPU cycles is proportional to the number of interfaces that must be polled.

Ethernet OAM has two major components:

- The *OAM client* establishes and manages Ethernet OAM on a link and enables and configures the OAM sublayer. During the OAM discovery phase, the OAM client monitors OAM PDUs received from the remote peer and enables OAM functionality. After the discovery phase, it manages the rules of response to OAM PDUs and the OAM remote loopback mode.
- The *OAM sublayer* presents two standard IEEE 802.3 MAC service interfaces facing the superior and inferior MAC sublayers. It provides a dedicated interface for the OAM client to pass OAM control information and PDUs to and from the client. The sublayer includes these components:
  - The *control block* provides the interface between the OAM client and other OAM sublayer internal blocks.
  - The *multiplexer* manages frames from the MAC client, the control block, and the parser and passes OAM PDUs from the control block and loopback frames from the parser to the subordinate layer.
  - The *parser* classifies frames as OAM PDUs, MAC client frames, or loopback frames and sends them to the appropriate entity: OAM PDUs to the control block, MAC client frames to the superior sublayer, and loopback frames to the multiplexer.

OAM Features

These OAM features are defined by IEEE 802.3ah:

- *Discovery* identifies devices in the network and their OAM capabilities. It uses periodic OAM PDUs to advertise OAM mode, configuration, and capabilities; PDU configuration; and platform identity. An optional phase allows the local station to accept or reject the configuration of the peer OAM entity.
- *Link monitoring* detects and indicates link faults under a variety of conditions and uses the event notification OAM PDU to notify the remote OAM device when it detects problems on the link. Error events include when the number of symbol errors, the number of frame errors, the number of frame errors within a specified number of frames, or the number of error seconds within a specified period exceeding a configured threshold.
- *Remote failure indication* conveys a slowly deteriorating quality of an OAM entity to its peers by communicating these conditions: Link Fault means a loss of signal, Dying Gasp means an unrecoverable condition, and Critical Event means an unspecified vendor-specific critical event. The switch can receive and process but not generate Link Fault or Critical Event OAM PDUs. It can

generate Dying Gasp OAM PDUs to show that Ethernet OAM is disabled, the interface is shut down, the interface enters the error-disabled state, or the switch is reloading. It can respond to, but not generate, Dying Gasp PDUs based on loss of power.

- *Remote loopback mode* ensures link quality with a remote peer during installation or troubleshooting. In this mode, when the switch receives a frame that is not an OAM PDU or a pause frame, it sends it back on the same port. The link appears to the user to be functioning. You can use the returned loopback acknowledgement to test delay, jitter, and throughput.

OAM Messages

Ethernet OAM messages or PDUs are standard length, untagged Ethernet frames between 64 and 1518 bytes. They do not go beyond a single hop and have a maximum transmission rate of 10 OAM PDUs per second. Message types are information, event notification, loopback control, or vendor-specific OAM PDUs.

Setting Up and Configuring Ethernet OAM

This section includes this information:

Default Ethernet OAM Configuration

The default configuration is as follows:

- Ethernet OAM is disabled on all interfaces.
- When Ethernet OAM is enabled on an interface, link monitoring is automatically turned on.
- Remote loopback is disabled.
- No Ethernet OAM templates are configured.

Ethernet OAM Configuration Guidelines

Follow these guidelines when configuring Ethernet OAM:

- The switch does not support monitoring of egress frames sent with cyclic redundancy code (CDC) errors. The **ethernet oam link-monitor transmit crc** interface-configuration or template-configuration commands are visible but are not supported on the switch. The commands are accepted but are not applied to an interface.

- For a remote failure indication, the switch does not generate Link Fault or Critical Event OAM PDUs. However, if these PDUs are received from a link partner, they are processed. The switch generates and receives Dying Gasp OAM PDUs when Ethernet OAM is disabled, the interface is shut down, the interface enters the error-disabled state, or the switch is reloading. It can respond to, but not generate, Dying Gasp PDUs based on loss of power.
- The switch does not support Ethernet OAM loopback on ports that belong to an EtherChannel, ISL trunk, and promiscuous trunk.

Enabling Ethernet OAM on an Interface

To enable Ethernet OAM on an interface, follow these steps:

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface** *interface-id*	Defines an interface to configure as an EOM interface, and enters interface configuration mode.
Step 3	**ethernet oam**	Enables Ethernet OAM on the interface.
Step 4	**ethernet oam** [**max-rate** *oampdus* | **min-rate** *seconds* | **mode** {**active** | **passive**} | **timeout** *seconds*]	Configures these optional OAM parameters: • (Optional) Enter **max-rate** *oampdus* to configure the maximum number of OAM PDUs sent per second. The range is from 1 to 10. • (Optional) Enter **min-rate** *seconds* to configure the minimum transmission rate in seconds when one OAM PDU is sent per second. The range is from 1 to 10. • (Optional) Enter **mode active** to set OAM client mode to active. **active** is the default. • (Optional) Enter **mode passive** to set OAM client mode to passive. **Note** When Ethernet OAM mode is enabled on two interfaces passing traffic, at least one must be in the active mode. • (Optional) Enter **timeout** *seconds* to set a time for OAM client timeout. The range is from 2 to 30.
Step 5	**end**	Returns to privileged EXEC mode.
Step 6	**show ethernet oam status** [**interface** *interface-id*]	Verifies the configuration.
Step 7	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

Enter the **no ethernet oam** interface configuration command to disable Ethernet OAM on the interface.

This example shows how to set basic OAM parameters on the switch:

```
Switch(config)# int gi1/3
Switch(config-if)# ethernet oam
Switch(config-if)# ethernet oam max-rate 9
Switch(config-if)# ethernet oam mode passive
Switch(config-if)# end
```

```
Switch# show ethernet oam status int gi1/2
GigabitEthernet1/2

General
-------
  Admin state:           enabled
  Mode:                  passive
  PDU max rate:          9 packets per second
  PDU min rate:          1 packet per 1 second
  Link timeout:          5 seconds
  High threshold action: no action
  Link fault action:     no action
  Dying gasp action:     no action
  Critical event action: no action

Link Monitoring
---------------
  Status: supported (on)

  Symbol Period Error
    Window:              100 x 1048576 symbols
    Low threshold:       1 error symbol(s)
    High threshold:      none

Frame Error
    Window:              10 x 100 milliseconds
    Low threshold:       1 error frame(s)
    High threshold:      none

  Frame Period Error
    Window:              1000 x 10000 frames
    Low threshold:       1 error frame(s)
    High threshold:      none

  Frame Seconds Error
    Window:              100 x 100 milliseconds
    Low threshold:       1 error second(s)
    High threshold:      none

  Receive-Frame CRC Error
    Window:              10 x 100 milliseconds
    Low threshold:       10 error frame(s)
    High threshold:      none

  Transmit-Frame CRC Error: Not Supported
```

Enabling Ethernet OAM Remote Loopback

You must enable Ethernet OAM remote loopback on an interface for the local OAM client to initiate OAM remote loopback operations. Changing this setting causes the local OAM client to exchange configuration information with its remote peer. Remote loopback is disabled by default.

Remote loopback has these limitations:

- Only data packets are looped back.
- You cannot configure Ethernet OAM remote loopback on ISL ports or ports that belong to an EtherChannel.
- Remote loopback can be supported on a max of 16 ports.

To enable Ethernet OAM remote loopback on an interface, follow these steps:

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface** *interface-id*	Defines an interface to configure as an EOM interface, and enters interface configuration mode.
Step 3	**ethernet oam remote-loopback** {**supported** | **timeout** *seconds*}	Enables Ethernet remote loopback on the interface or set a loopback timeout period. • Enter **supported** to enable remote loopback. • Enter **timeout** *seconds* to set a remote loopback timeout period. The range is from 1 to 10 seconds.
Step 4	**end**	Returns to privileged EXEC mode.
Step 5	**ethernet oam remote-loopback** {**start** | **stop**} {**interface** *interface-id*}	Turns on or turn off Ethernet OAM remote loopback on an interface.
Step 6	**show ethernet oam status** [**interface** *interface-id*]	Verifies the configuration.
Step 7	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

Use the **no ethernet oam remote-loopback** {**supported** | **timeout**} interface configuration command to disable remote loopback support or remove the timeout setting.

This example shows how to enable OAM Remote Loopback:

```
Switch(config)# int gi1/3
Switch(config-if)# ethernet oam
Switch(config-if)# ethernet oam remote-loopback supported
Switch(config-if)# end
Switch# show running int gi1/1
Building configuration...

Current configuration : 209 bytes
!
interface GigabitEthernet1/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,19
 switchport mode trunk
 ethernet oam remote-loopback supported
 ethernet oam
end

Switch# ethernet oam remote-loopback start int gi1/1
This is a intrusive loopback.
Therefore, while you test Ethernet OAM MAC connectivity,
you will be unable to pass traffic across that link.
Proceed with Remote Loopback? [confirm]

Switch# ethernet oam remote-loopback stop int gi1/1
Switch#
*Apr  9 12:52:39.793: %ETHERNET_OAM-6-LOOPBACK: Interface Gi1/1 has exited the master
loopback mode.
```

Configuring Ethernet OAM Link Monitoring

You can configure high and low thresholds for link-monitoring features. If no high threshold is configured, the default is **none**—no high threshold is set. If you do not set a low threshold, the default is a value lower than the high threshold.

Cisco does not generate link event PDUs for rxcrc and trxcrc errors because these are nonstandard.

To configure Ethernet OAM link monitoring on an interface, follow these steps:

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface** *interface-id*	Defines an interface, and enters interface configuration mode.
Step 3	**ethernet oam link-monitor supported**	Enables the interface to support link monitoring. This is the default. You need to enter this command only if it has been disabled by previously entering the **no ethernet oam link-monitor supported** command.
Step 4	**ethernet oam link-monitor symbol-period** {**threshold** {**high** {*high symbols* | **none**} | **low** {*low-symbols*}} | **window** *symbols*} Repeat this step to configure both high and low thresholds.	(Optional) Configures high and low thresholds for an error-symbol period that trigger an error-symbol period link event. • Enter **threshold high** *high-symbols* to set a high threshold in number of symbols. The range is 1 to 65535. The default is **none**. • Enter **threshold high none** to disable the high threshold if it was set. This is the default. • Enter **threshold low** *low-symbols* to set a low threshold in number of symbols. The range is 0 to 65535. It must be lower than the high threshold. • Enter **window** *symbols* to set the window size (in number of symbols) of the polling period. The range is 1 to 65535 symbols.
Step 5	**ethernet oam link-monitor frame** {**threshold** {**high** {*high-frames* | **none**} | **low** {*low-frames*}} | **window** *milliseconds*} Repeat this step to configure both high and low thresholds.	(Optional) Configures high and low thresholds for error frames that trigger an error-frame link event. • Enter **threshold high** *high-frames* to set a high threshold in number of frames. The range is 1 to 65535. The default is **none**. • Enter **threshold high none** to disable the high threshold if it was set. This is the default. • Enter **threshold low** *low-frames* to set a low threshold in number of frames. The range is 0 to 65535. The default is 1. • Enter **window** *milliseconds* to set the a window and period of time during which error frames are counted. The range is 10 to 600 and represents the number of milliseconds in multiples of 100. The default is 100.

	Command	Purpose
Step 6	**ethernet oam link-monitor frame-period** {**threshold** {**high** {*high-frames* | **none**} | **low** {*low-frames*}} | **window** *frames*} Repeat this step to configure both high and low thresholds.	(Optional) Configures high and low thresholds for the error-frame period that triggers an error-frame-period link event. • Enter **threshold high** *high-frames* to set a high threshold in number of frames. The range is 1 to 65535. The default is **none**. • Enter **threshold high none** to disable the high threshold if it was set. This is the default. • Enter **threshold low** *low-frames* to set a low threshold in number of frames. The range is 0 to 65535. The default is 1. • Enter **window** *frames* to set the a polling window size in number of frames. The range is 1 to 65535; each value is a multiple of 10000 frames. The default is 1000.
Step 7	**ethernet oam link-monitor frame-seconds** {**threshold** {**high** {*high-frames* | **none**} | **low** {*low-frames*}} | **window** *milliseconds*} Repeat this step to configure both high and low thresholds.	(Optional) Configures high and low thresholds for the frame-seconds error that triggers an error-frame-seconds link event. • Enter **threshold high** *high-frames* to set a high error frame-seconds threshold in number of seconds. The range is 1 to 900. The default is none. • Enter **threshold high none** to disable the high threshold if it was set. This is the default. • Enter **threshold low** *low-frames* to set a low threshold in number of frames. The range is 1 to 900. The default is 1. • Enter **window** *frames* to set the a polling window size in number of milliseconds. The range is 100 to 9000; each value is a multiple of 100 milliseconds. The default is 1000.

	Command	Purpose
Step 8	**ethernet oam link-monitor receive-crc** {**threshold** {**high** {*high-frames* | **none**} | **low** {*low-frames*}} | **window** *milliseconds*} Repeat this step to configure both high and low thresholds.	(Optional) Configures thresholds for monitoring ingress frames received with cyclic redundancy code (CRC) errors for a period of time. • Enter **threshold high** *high-frames* to set a high threshold for the number of frames received with CRC errors. The range is 1 to 65535 frames. • Enter **threshold high none** to disable the high threshold. • Enter **threshold low** *low-frames* to set a low threshold in number of frames. The range is 0 to 65535. The default is 1. • Enter **window** *milliseconds* to set the a window and period of time during which frames with CRC errors are counted. The range is 10 to 1800 and represents the number of milliseconds in multiples of 100. The default is 100.
Step 9	[**no**] **ethernet link-monitor on**	(Optional) Starts or stop (when the **no** keyword is entered) link-monitoring operations on the interface. Link monitoring operations start automatically when support is enabled.
Step 10	**end**	Returns to privileged EXEC mode.
Step 11	**show ethernet oam status** [**interface** *interface-id*]	Verifies the configuration.
Step 12	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

The **ethernet oam link-monitor transmit-crc** {**threshold** {**high** {*high-frames* | **none**} | **low** {*low-frames*}} | **window** *milliseconds*} command is visible on the switch and you can enter it, but it is not supported. Enter the **no** form of the command to disable the configuration. Use the **no** form of each command to disable the threshold setting.

Symbol error counters are supported on the following line cards and supervisor cards:

- Supervisor cards: WS-X4515, WS-X4516, WS-X4013+, WS-X4013+TS, WS-X4516-10GE, WS-X4013+10GE
- Line cards: WS-X4148-RJ, WS-X4124-RJ, WS-X4232, WS-X4232-RJ-XX, WS-X4148-RJ21, WS-X4504-FX-MT, WS-X4224-RJ21-XX, WS-X4124-FX-MT, WS-X4232-L3

The rest of the cards do not support symbol error counters.

Configuring Ethernet OAM Remote Failure Indications

You can configure an error-disable action to occur on an interface when the following occur:

- crossing the high thresholds configured on the interface for link monitoring
- on reception of Dying Gasp, executing **shut** on the interface
- on reception of Dying Gasp, **executing reload** command
- on reception of Dying Gasp, **executing no ethernet oam** command on the interface

To enable Ethernet OAM remote-failure indication actions on an interface, follow these steps:

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface** *interface-id*	Defines an interface and enters interface configuration mode.
Step 3	**ethernet oam remote-failure** [**dying-gasp**] **action error-disable-interface**	Configures the Ethernet OAM remote-failure action on the interface. You can configure disabling the interface by selecting **dying-gasp** to shut down the interface when Ethernet OAM is disabled or the interface enters the error-disabled state.
Step 4	**end**	Returns to privileged EXEC mode.
Step 5	**show ethernet oam status** [**interface** *interface-id*]	Verifies the configuration.
Step 6	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

This example shows how to configure Ethernet OAM remote-failure action on the switch interface:

```
Switch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# int gi1/1
Switch(config-if)# ethernet oam remote-failure dying-gasp action error
Switch(config-if)# ethernet oam link-monitor high-threshold action error
Switch(config-if)# end
Switch# show running-config int gi1/1
Building configuration...

Current configuration : 353 bytes
!
interface GigabitEthernet1/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,19
 switchport mode trunk
 ethernet oam remote-loopback supported
 ethernet oam link-monitor high-threshold action error-disable-interface
 ethernet oam remote-failure dying-gasp action error-disable-interface
 ethernet oam
end
Switch# show ethernet oam status int gi1/1
GigabitEthernet1/1
General
-------
  Admin state:           enabled
  Mode:                  active
  PDU max rate:          10 packets per second
  PDU min rate:          1 packet per 1 second
  Link timeout:          5 seconds
  High threshold action: error disable interface
  Link fault action:     no action
  Dying gasp action:     error disable interface
  Critical event action: no action

Link Monitoring
---------------
  Status: supported (on)

  Symbol Period Error
```

```
    Window:              100 x 1048576 symbols
    Low threshold:       1 error symbol(s)
    High threshold:      none

  Frame Error
    Window:              10 x 100 milliseconds
    Low threshold:       1 error frame(s)
    High threshold:      none

  Frame Period Error
    Window:              1000 x 10000 frames
    Low threshold:       1 error frame(s)
    High threshold:      none

  Frame Seconds Error
    Window:              100 x 100 milliseconds
    Low threshold:       1 error second(s)
    High threshold:      none

  Receive-Frame CRC Error
    Window:              10 x 100 milliseconds
    Low threshold:       10 error frame(s)
    High threshold:      none

  Transmit-Frame CRC Error: Not Supported
```

To enable Ethernet OAM failover action on an EtherChannel interface, follow these steps:

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface port-channel** *interface-id*	Defines an interface and enters interface configuration mode.
Step 3	**switchport mode** *mode*	Configures the mode of the EtherChannel interface.
Step 4	**ethernet oam link-monitor high-threshold action failover**	Configures the Ethernet OAM remote-failure action on the port channel interface to failover. This action is configurable only for link monitoring RFI. If failover is configured on the EtherChannel interface, the interface is not error-disabled if it is the last member port of the EtherChannel.
Step 5	**end**	Returns to privileged EXEC mode.
Step 6	**show ethernet oam status** [**interface** *interface-id*]	Verifies the configuration.
Step 7	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

The switch does not generate Link Fault or Critical Event OAM PDUs. However, if these PDUs are received from a link partner, they are processed. The switch supports sending and receiving Dying Gasp OAM PDUs when Ethernet OAM is disabled, the interface is shut down, the interface enters the error-disabled state, or the switch is reloading. It can respond to but not generate Dying Gasp PDUs based on loss of power. Enter the **no ethernet remote-failure** {**critical-event** | **dying-gasp** | **link-fault**} **action** command to disable the remote failure indication action.

Configuring Ethernet OAM Templates

You can create a template for configuring a common set of options on multiple Ethernet OAM interfaces. The template can be configured to monitor frame errors, frame-period errors, frame-second errors, received CRS errors, and symbol-period errors and thresholds. You can also set the template to put the interface in error-disabled state if any high thresholds are exceeded. These steps are optional and can be performed in any sequence or repeated to configure different options.

To configure an Ethernet OAM template and to associate it with an interface, follow these steps:

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**template** *template-name*	Creates a template and enters template configuration mode.
Step 3	**ethernet oam link-monitor receive-crc** {**threshold** {**high** {*high-frames* | **none**} | **low** {*low-frames*}} | **window** *milliseconds*}	(Optional) Configures thresholds for monitoring ingress frames received with cyclic redundancy code (CRC) errors for a period of time. • Enter **threshold high** *high-frames* to set a high threshold for the number of frames received with CRC errors. The range is 1 to 65535 frames. • Enter **threshold high none** to disable the high threshold. • Enter **threshold low** *low-frames* to set a low threshold in number of frames. The range is 0 to 65535. The default is 1. • Enter **window** *milliseconds* to set the a window and period of time during which frames with CRC errors are counted. The range is 10 to 1800 and represents the number of milliseconds in multiples of 100. The default is 100.
Step 4	**ethernet oam link-monitor symbol-period** {**threshold** {**high** {*high symbols* / **none**} | **low** {*low-symbols*}} | **window** *symbols*}	(Optional) Configures high and low thresholds for an error-symbol period that triggers an error-symbol period link event. • Enter **threshold high** *high-symbols* to set a high threshold in number of symbols. The range is 1 to 65535. • Enter **threshold high none** to disable the high threshold. • Enter **threshold low** *low-symbols* to set a low threshold in number of symbols. The range is 0 to 65535. It must be lower than the high threshold. • Enter **window** *symbols* to set the window size (in number of symbols) of the polling period. The range is 1 to 65535 symbols.

	Command	Purpose
Step 5	**ethernet oam link-monitor frame** {**threshold** {**high** {*high-frames* | **none**} | **low** {*low-frames*}} | **window** *milliseconds*}	(Optional) Configures high and low thresholds for error frames that trigger an error-frame link event. • Enter **threshold high** *high-frames* to set a high threshold in number of frames. The range is 1 to 65535. You must enter a high threshold. • Enter **threshold high none** to disable the high threshold. • Enter **threshold low** *low-frames* to set a low threshold in number of frames. The range is 0 to 65535. The default is 1. • Enter **window** *milliseconds* to set the a window and period of time during which error frames are counted. The range is 10 to 600 and represents the number of milliseconds in a multiple of 100. The default is 100.
Step 6	**ethernet oam link-monitor frame-period** {**threshold** {**high** {*high-frames* | **none**} | **low** {*low-frames*}} | **window** *frames*}	(Optional) Configures high and low thresholds for the error-frame period that triggers an error-frame-period link event. • Enter **threshold high** *high-frames* to set a high threshold in number of frames. The range is 1 to 65535. You must enter a high threshold. • Enter **threshold high none** to disable the high threshold. • Enter **threshold low** *low-frames* to set a low threshold in number of frames. The range is 0 to 65535. The default is 1. • Enter **window** *frames* to set the a polling window size in number of frames. The range is 1 to 65535; each value is a multiple of 10000 frames. The default is 1000.
Step 7	**ethernet oam link-monitor frame-seconds** {**threshold** {**high** {*high-seconds* | **none**} | **low** {*low-seconds*}} | **window** *milliseconds*}	(Optional) Configures frame-seconds high and low thresholds for triggering an error-frame-seconds link event. • Enter **threshold high** *high-seconds* to set a high threshold in number of seconds. The range is 1 to 900. You must enter a high threshold. • Enter **threshold high none** to disable the high threshold. • Enter **threshold low** *low-frames* to set a low threshold in number of frames. The range is 1 to 900. The default is 1. • Enter **window** *frames* to set the a polling window size in number of frames. The range is 100 to 9000; each value is a multiple of 100 milliseconds. The default is 1000.

	Command	Purpose
Step 8	**ethernet oam link-monitor high threshold action error-disable-interface**	(Optional) Configures the switch to put an interface in an error disabled state when a high threshold for an error is exceeded.
Step 9	**exit**	Returns to global configuration mode.
Step 10	**interface** *interface-id*	Defines an Ethernet OAM interface and enters interface configuration mode.
Step 11	source-template *template-name*	Associates the template to apply the configured options to the interface.
Step 12	**end**	Returns to privileged EXEC mode.
Step 13	**show ethernet oam status** [**interface** *interface-id*]	Verifies the configuration.
Step 14	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

The switch does not support monitoring egress frames with CRC errors. The **ethernet oam link-monitor transmit-crc** {**threshold** {**high** {*high-frames* | **none**} | **low** {*low-frames*}} | **window** *milliseconds*} command is visible on the switch and you can enter it, but it is not supported. Use the **no** form of each command to remove the option from the template. Use the **no source-template** *template-name* command to remove the source template association.

The following example illustrates how to configure an Ethernet OAM template and to associate it with an interface:

```
Switch# conf t
Switch(config)# template oam
Switch(config-template)# ethernet oam link-monitor receive-crc threshold high 1000
Switch(config-template)# ethernet oam link-monitor receive-crc threshold low 10
Switch(config-template)# ethernet oam link-monitor symbol-period threshold high 5000
Switch(config-template)# ethernet oam link-monitor symbol-period threshold low 5
Switch(config-template)# ethernet oam link-monitor frame threshold high 8000
Switch(config-template)# ethernet oam link-monitor frame threshold low 8
Switch(config-template)# ethernet oam link-monitor frame-period threshold hig 9000
Switch(config-template)# ethernet oam link-monitor frame-period threshold low 9
Switch(config-template)# ethernet oam link-monitor high action error-disable-interface
Switch(config-template)# exit
Switch(config)# int gi1/2
Switch(config-if)# source template oam
Switch(config-if)# end
Switch# show ethernet oam status int gi1/2
GigabitEthernet1/2
General
-------
  Admin state:           enabled
  Mode:                  active
  PDU max rate:          10 packets per second
  PDU min rate:          1 packet per 1 second
  Link timeout:          5 seconds
  High threshold action: error disable interface
  Link fault action:     no action
  Dying gasp action:     no action
  Critical event action: no action
```

```
Link Monitoring
---------------
  Status: supported (on)

  Symbol Period Error
    Window:              100 x 1048576 symbols
    Low threshold:       5 error symbol(s)
    High threshold:      5000 error symbol(s)

  Frame Error
    Window:              10 x 100 milliseconds
    Low threshold:       8 error frame(s)
    High threshold:      8000 error frame(s)

  Frame Period Error
    Window:              1000 x 10000 frames
    Low threshold:       9 error frame(s)
    High threshold:      9000 error frame(s)

  Frame Seconds Error
    Window:              100 x 100 milliseconds
    Low threshold:       1 error second(s)
    High threshold:      none

  Receive-Frame CRC Error
    Window:              10 x 100 milliseconds
    Low threshold:       10 error frame(s)
    High threshold:      1000 error frame(s)

  Transmit-Frame CRC Error: Not Supported
```

Displaying Ethernet OAM Protocol Information

To display Ethernet OAM protocol information, you can use the privileged EXEC commands in Table 53-3.

Table 53-3 Displaying Ethernet OAM Protocol Information

Command	Purpose
`show ethernet oam discovery [interface interface-id]`	Displays discovery information for all Ethernet OAM interfaces or the specified interface.
`show ethernet oam statistics [interface interface-id]`	Displays detailed information about Ethernet OAM packets.
`show ethernet oam status [interface interface-id]`	Displays Ethernet OAM configuration for all interfaces or the specified interface.
`show ethernet oam summary`	Displays active Ethernet OAM sessions on the switch.

These examples show how to apply these commands:

```
Switch# show ethernet oam discovery
GigabitEthernet1/1
Local client
------------
  Administrative configurations:
    Mode:              active
    Unidirection:      not supported
```

```
    Link monitor:      supported (on)
    Remote loopback:   supported
    MIB retrieval:     not supported
    Mtu size:          1500

  Operational status:
    Port status:       operational
    Loopback status:   no loopback
    PDU revision:      10

Remote client
-------------
  MAC address: 000f.8f03.3591
  Vendor(oui): 00000C(cisco)

  Administrative configurations:
    PDU revision:      2
    Mode:              active
    Unidirection:      not supported
    Link monitor:      supported
    Remote loopback:   supported
    MIB retrieval:     not supported
    Mtu size:          1500

Switch# show ethernet oam statistics
GigabitEthernet1/1
Counters:
---------
  Information OAMPDU Tx                   : 101163
  Information OAMPDU Rx                   : 51296
  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              : 12
  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
  Cisco OAMPDU Tx                         : 7
  Cisco OAMPDU Rx                         : 8
  Unsupported OAMPDU Tx                   : 0
  Unsupported OAMPDU Rx                   : 0
  Frames Lost due to OAM                  : 0

Local Faults:
-------------
  0 Link Fault records
  2 Dying Gasp records
    Total dying gasps       : 7
    Time stamp              : 1d01h

    Total dying gasps       : 6
    Time stamp              : 1d01h

  0 Critical Event records

Remote Faults:
--------------
  0 Link Fault records
  2 Dying Gasp records
```

```
    Total dying gasps       : 8
    Time stamp              : 1d01h

    Total dying gasps       : 7
    Time stamp              : 1d01h

  0 Critical Event records

Local event logs:
-----------------
  0 Errored Symbol Period records
  0 Errored Frame records
  0 Errored Frame Period records
  0 Errored Frame Second records

Remote event logs:
------------------
  0 Errored Symbol Period records
  0 Errored Frame records
  0 Errored Frame Period records
  0 Errored Frame Second records


Switch# show ethernet oam summary
Symbols:          * - Master Loopback State,  # - Slave Loopback State
                  & - Error Block State
Capability codes: L - Link Monitor,  R - Remote Loopback
                  U - Unidirection,  V - Variable Retrieval
  Local                         Remote
Interface       MAC Address    OUI    Mode    Capability

  Gi1/1         000f.8f03.3591 00000C active   L R
```

Ethernet CFM and Ethernet OAM Interaction

You can also configure the OAM Manager infrastructure to interact between CFM and Ethernet OAM. When the Ethernet OAM protocol is running on an interface that has CFM MEPs configured, Ethernet OAM informs CFM of the state of the interface. Interaction is unidirectional from the Ethernet OAM to the CFM protocol, and the only information exchanged is the user network interface port status.

The Ethernet OAM protocol notifies CFM when these conditions occur:

- Error thresholds are crossed at the local interface.

  CFM responds to the notification by sending a port status of *Local_Excessive_Errors* in the Port StatusType Length Value (TLV).

- Ethernet OAM receives an OAM PDU from the remote side showing that an error threshold is exceeded on the remote endpoint.

  CFM responds to the notification by sending a port status of *Remote_Excessive_Errors* in the Port Status TLV.

- The local port is set into loopback mode.

  CFM responds by sending a port status of Test in the Port Status TLV.

- The remote port is set into loopback mode.

  CFM responds by sending a port status of Test in the Port Status TLV.

For more information about CFM and interaction with Ethernet OAM, see the Ethernet Connectivity Fault Management feature module at this URL:

http://www.cisco.com/en/US/docs/ios/12_2sr/12_2sra/feature/guide/srethcfm.html

Ethernet OAM and CFM Configuration Example

These are configuration example of the interworking between Ethernet OAM and CFM in a sample service provider network. Such a hypothetical network would contain a provider-edge switch connected to a customer edge switch at each endpoint. You must configure CFM, E-LMI, and Ethernet OAM between the customer edge and the provider edge switch.

Customer-edge switch 1 (CE1) configuration:

```
Switch# config t
Switch(config)# interface GigabitEthernet1/1
Switch(config-if)# switchport trunk allowed vlan 10
Switch(config-if)# switchport mode trunk
Switch(config-if)# ethernet oam remote-loopback supported
Switch(config-if)# ethernet oam
Switch(config-if)# exit
```

Provider-edge switch 1 (PE1) configuration:

```
Switch# config t
Switch(config)# interface FastEthernet1/20
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# ethernet cfm mip level 7
Switch(config-if)# ethernet cfm mep level 4 mpid 100 vlan 100
Switch(config-if)# ethernet oam remote-loopback supported
Switch(config-if)# ethernet oamt
```

Provider-edge switch 2 (PE2) configuration:

```
Switch# config t
Switch(config)# interface GigabitEthernet1/20
Switch(config-if)# switchport mode trunk
Switch(config-if)# ethernet cfm mip level 7
Switch(config-if)# ethernet cfm mep level 4 mpid 101 vlan 10
Switch(config-if)# ethernet oam remote-loopback supported
Switch(config-if)# ethernet oam
```

Customer-edge switch 2 (CE2) configuration:

```
Switch# config t
Switch(config)# interface GigabitEthernet1/1
Switch(config-if)# switchport trunk allowed vlan 10
Switch(config-if)# switchport mode trunk
Switch(config-if)# ethernet oam remote-loopback supported
Switch(config-if)# ethernet oam
Switch(config-if)# exit
```

These output examples show provider-edge switch port status of the configuration. Port status shows as *UP* at both switches.

Switch PE1:

```
Switch# show ethernet cfm maintenance points remote
MPID  Level Mac Address    Vlan PortState InGressPort     Age(sec) Service ID
101 * 4     0015.633f.6900 10   UP        Gi1/1         27       blue
```

Switch PE2:

```
Switch# show ethernet cfm maintenance points remote
MPID  Level Mac Address    Vlan PortState InGressPort     Age(sec) Service ID
100 * 4     0012.00a3.3780 10   UP        Gi1/1         8        blue
Total Remote MEPs: 1
```

This example shows the output when you start remote loopback on CE1 (or PE1). The port state on the remote PE switch shows as *Test* and the remote CE switch enters into error-disable mode.

```
Switch# ethernet oam remote-loopback start interface gigabitethernet 1/1
This is a intrusive loopback.
Therefore, while you test Ethernet OAM MAC connectivity,
you will be unable to pass traffic across that link.
Proceed with Remote Loopback? [confirm]
```

Switch PE1:

```
Switch# show ethernet cfm maintenance points remote
MPID  Level Mac Address    Vlan PortState InGressPort     Age(sec) Service ID
101 * 4     0015.633f.6900 10   UP        Gi1/1         27       blue
```

Switch PE2:

```
Switch# show ethernet cfm maintenance points remote
MPID  Level Mac Address    Vlan PortState InGressPort     Age(sec) Service ID
100 * 4     0012.00a3.3780 10   TEST      Gi1/1         8        blue
Total Remote MEPs: 1
```

In addition, if you shut down the CE1 interface that connects to PE1, the remote PE2 port shows a PortState of *Down*.