



CHAPTER 41

Configuring Ethernet OAM, CFM, and E-LMI

Ethernet Operations, Administration, and Maintenance (OAM) is a protocol for installing, monitoring, and troubleshooting Ethernet networks to increase management capability within the context of the overall Ethernet infrastructure. The Catalyst 3750 Metro switch supports IEEE 802.1ag Connectivity Fault Management (CFM), Ethernet Local Management Interface (E-LMI), and IEEE 802.3ah Ethernet OAM discovery, link monitoring, remote fault detection, and remote loopback. Cisco IOS Release 12.2(40)SE adds support for IP Service Level Agreements (SLAs) for CFM. Ethernet OAM manager controls the interworking between any two of the protocols (CFM, E-LMI, and OAM).

This chapter provides information about configuring CFM, E-LMI, and the Ethernet OAM protocol.

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

http://www.cisco.com/en/US/products/ps6922/products_feature_guide09186a008066fcb8.html

For E-LMI configuration and commands see this URL:

http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a0080690f2d.html

For complete syntax of the Ethernet OAM manager commands used in this chapter to configure CFM and E-LMI interaction, see the command reference for this release.

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

http://www.cisco.com/en/US/products/ps6922/products_feature_guide09186a008067344c.html

For documentation for the CFM and Ethernet OAM commands, see this URL:

http://www.cisco.com/en/US/docs/ios/cether/command/reference/ce_book.html

This chapter contains these sections:

- [Understanding Ethernet CFM, page 41-2](#)
- [Configuring Ethernet CFM, page 41-5](#)
- [Displaying Ethernet CFM Information, page 41-13](#)
- [Understanding the Ethernet OAM Protocol, page 41-14](#)
- [Setting Up and Configuring Ethernet OAM, page 41-15](#)
- [Displaying Ethernet OAM Protocol Information, page 41-24](#)
- [Understanding E-LMI, page 41-24](#)
- [Configuring E-LMI, page 41-26](#)
- [Displaying E-LMI and OAM Manager Information, page 41-31](#)
- [Ethernet CFM and Ethernet OAM Interaction, page 41-32](#)

Understanding Ethernet CFM

Ethernet CFM is an end-to-end per-service-instance (per VLAN) Ethernet layer OAM protocol that 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 check 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. E-LMI is confined between the user provider-edge (UPE) and the CE device and relies on CFM for reporting status of the metro-Ethernet network to the customer-edge device.

These sections contain conceptual information about Ethernet CFM:

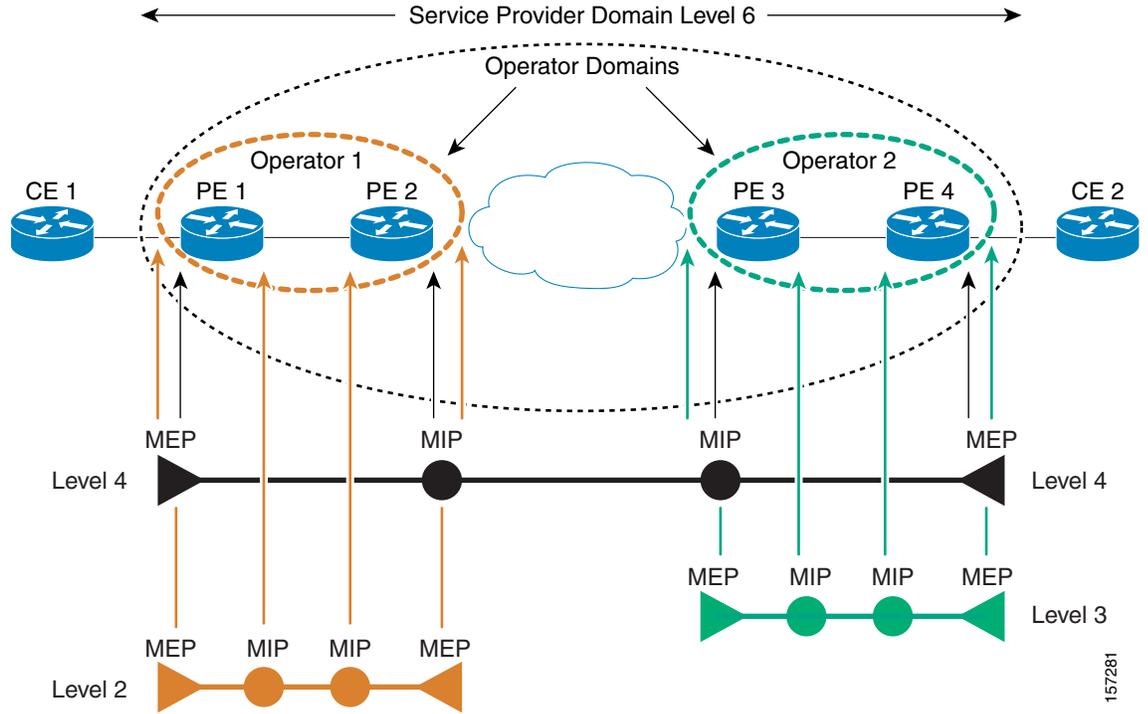
- [CFM Domain, page 41-2](#)
- [Maintenance Points, page 41-3](#)
- [CFM Messages, page 41-4](#)
- [Crosscheck Function, page 41-4](#)
- [SNMP Traps, page 41-4](#)
- [IP SLAs Support for CFM, page 41-4](#)

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 ports internal to it, but at its boundary. You assign a unique maintenance level (from 0 to 7) to define the hierarchical relationship between domains. The larger the domain, the higher the level. For example, as shown in [Figure 41-1](#), 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 is 3 or 4.

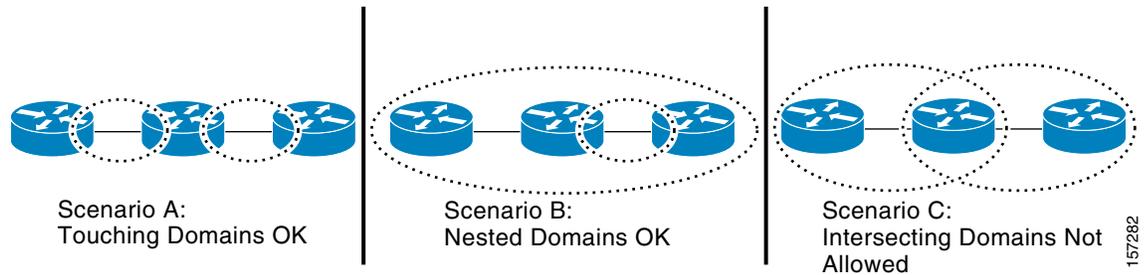
As shown in [Figure 41-2](#), domains cannot intersect or overlap because that would require management by more than one entity, which is not allowed. Domains can touch or nest (if the outer domain has a higher maintenance level than the nested domain). Nesting domains is useful when a service provider contract 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 a per-domain basis.

Figure 41-1 CFM Maintenance Domains



157281

Figure 41-2 Allowed Domain Relationships



157282

Maintenance Points

A maintenance point is a demarcation point on an interface that participates in CFM within a maintenance domain. 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 inward-facing points at the edge of the domain that define the boundary and confine CFM messages within these boundaries. *Inward facing* means that they communicate through the relay function side, not the wire side (connected to the port). A MEP sends and receives CFM frames through the relay function. It drops all CFM frames of 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, regardless of 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).

- Maintenance intermediate points (MIPs) are internal to 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, regardless of whether they are received from the relay or wire side.

If port on which the MEP is configured is blocked by Spanning-Tree Protocol (STP), the port cannot receive or transmit CFM messages. 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 and respond to CFM messages from the wire side.

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). These 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 configured 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 if 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.

Crosscheck Function

The crosscheck function is a timer-driven post-provisioning service verification 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 SNMP traps: CC traps and crosscheck traps. Supported CC traps are MEP up, MEP down, cross-connect (a service ID does not match the VLAN), loop, and configuration error. The crosscheck traps are service up, MEP missing (an expected MEP is down), and unknown MEP.

IP SLAs Support for CFM

Starting with Cisco IOS Release 12.2(40)SE, the switch supports CFM with IP Service Level Agreements (SLAs), which provides the ability to gather 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 SLAs operations and use Simple Network Management Protocol (SNMP) trap notifications and syslog messages for proactive threshold violation monitoring.

For more information about IP SLAs, see [Chapter 39, “Configuring Cisco IOS IP SLAs Operations.”](#)

IP SLAs 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 SLAs operations that provide performance metrics for only the IP layer, IP SLAs with CFM provides performance metrics for Layer 2.

You can manually configure individual Ethernet ping or jitter operations. You can also configure an IP SLAs 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 SLAs operation with CFM, see the *IP SLAs for Metro-Ethernet* feature module at this URL:

http://www.cisco.com/en/US/products/ps6922/products_feature_guide09186a00807d72f5.html

Configuring Ethernet CFM

Configuring Ethernet CFM requires preparing the network and configuring services. You can optionally configure and enable crosschecking. These sections are included

- [Default Ethernet CFM Configuration, page 41-5](#)
- [Ethernet CFM Configuration Guidelines, page 41-5](#)
- [Preparing the Ethernet CFM Network, page 41-6](#)
- [Configuring Ethernet CFM Service, page 41-7](#)
- [Configuring Ethernet CFM Crosscheck, page 41-8](#)
- [Configuring IP SLAs CFM Operation, page 41-9](#)

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 ports 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:

- CFM is not supported and cannot be configured on routed ports.
- Starting with Cisco IOS Release 12.2(40)SE, 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 on private VLAN ports. The configuration is allowed, but does not take effect.

Preparing the Ethernet CFM Network

Beginning in privileged EXEC mode, follow these steps to prepare the network for Ethernet CFM:

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>ethernet cfm traceroute cache [size <i>entries</i> hold-time <i>minutes</i>]</code>	(Optional) Configure the CFM traceroute cache. You can set a maximum cache size or hold time. <ul style="list-style-type: none"> (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 3	<code>ethernet cfm domain <i>domain-name</i> level <i>level-id</i></code>	Define 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.
Step 4	<code>mep archive-hold-time <i>minutes</i></code>	(Optional) Set 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 5	<code>exit</code>	Return to global configuration mode.
Step 6	<code>interface <i>interface-id</i></code>	Specify a physical interface or a port channel to configure, and enter interface configuration mode.
Step 7	<code>ethernet cfm mip level <i>level-id</i></code>	Configure an operator-level maintenance intermediate point (MIP) for the domain level-ID defined in Step 3. <p>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.</p>
Step 8	<code>exit</code>	Return to global configuration mode.
Step 9	<code>ethernet cfm cc {[enable] level {<i>level-id</i> any} vlan {<i>vlan-id</i> any}}</code>	Configure per domain continuity check (cc) parameters. The level ID identifies the domain to which configuration applies. <ul style="list-style-type: none"> 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 10	<code>end</code>	Return to privileged EXEC mode.
Step 11	<code>show ethernet cfm domain brief</code> <code>show ethernet cfm maintenance-points local</code> <code>show ethernet cfm traceroute-cache</code>	Verify the configuration.

	Command	Purpose
Step 12	<code>show running-config</code>	Verify your entries.
Step 13	<code>copy running-config startup-config</code>	(Optional) Save 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 Service

Beginning in privileged EXEC mode, follow these steps to set up service for Ethernet CFM:

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>ethernet cfm domain <i>domain-name</i> level <i>level-id</i></code>	Define 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.
Step 3	<code>service <i>csi-id</i> vlan <i>vlan-id</i></code>	Define a universally unique customer service instance (CSI) and VLAN ID within the maintenance domain. <ul style="list-style-type: none"> <i>csi-id</i>—a string of no more than 100 characters that identifies the CSI. <i>vlan-id</i>—VLAN range is from 1 to 4095. You cannot use the same VLAN ID for more than one domain at the same level.
Step 4	<code>exit</code>	Return to global configuration mode.
Step 5	<code>ethernet cfm enable</code>	Globally enable CFM.
Step 6	<code>interface <i>interface-id</i></code>	Specify a physical interface or a port channel to configure, and enter interface configuration mode.
Step 7	<code>ethernet cfm mip level <i>level-id</i></code>	Configure a customer level or service-provider level maintenance intermediate point (MIP) for the interface. The MIP level range is 0 to 7. <p>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.</p>

	Command	Purpose
Step 8	ethernet cfm mep level <i>level-id</i> [inward] mpid identifier vlan <i>vlan-id</i>	Configure maintenance end points (MEPs). for different maintenance levels. The MEP level range is 0 to 7. <ul style="list-style-type: none"> (Optional) Specify the end point in the 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 <i>vlan-id</i>, 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 9	exit	Return to global configuration mode.
Step 10	snmp-server enable traps ethernet cfm cc [mep-up] [mep-down] [config] [loop] [cross-connect]	(Optional) Enable Ethernet CFM continuity check traps.
Step 11	snmp-server enable traps ethernet cfm crosscheck [mep-unknown] [mep-missing] [service-up]	(Optional) Enable Ethernet CFM crosscheck traps.
Step 12	end	Return to privileged EXEC mode.
Step 13	show ethernet cfm { domain maintenance-points }	Verify the configuration.
Step 14	show running-config	Verify your entries.
Step 15	copy running-config startup-config	(Optional) Save 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 Ethernet CFM Crosscheck

Beginning in privileged EXEC mode, follow these steps to configure Ethernet CFM crosscheck:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ethernet cfm mep crosscheck start-delay <i>delay</i>	Configure 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	ethernet cfm domain <i>domain-name</i> level <i>level-id</i>	Define 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.

	Command	Purpose
Step 4	mep crosscheck mpid <i>identifier</i> vlan <i>vlan-id</i> [mac <i>remote MAC address</i>]	Define a remote maintenance end point (MEP) within a maintenance domain. <ul style="list-style-type: none"> For mpid <i>identifier</i>, enter a maintenance end point identifier. The identifier must be unique for each VLAN (service instance). The range is 1 to 8191. For vlan <i>vlan-id</i>, the VLAN range is from 1 to 4095. (Optional) Specify the MAC address of the remote MEP.
Step 5	end	Return to privileged EXEC mode.
Step 6	ethernet cfm mep crosscheck { enable disable } level <i>level-id</i> vlan { <i>vlan-id</i> any }	Enable or disable CFM crosscheck for one or more maintenance levels and VLANs. <ul style="list-style-type: none"> For level <i>level-id</i>, 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 <i>vlan-id</i>, enter the 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 commas, or enter any for any VLAN.
Step 7	end	Return to privileged EXEC mode.
Step 8	show ethernet cfm maintenance-points remote crosscheck	Verify the configuration.
Step 9	show ethernet cfm errors	Enter this command after you enable CFM crosscheck to display the results of the crosscheck operation.
Step 10	copy running-config startup-config	(Optional) Save 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 individual IP SLAs 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 3750 Metro switch for a class of service (CoS) probe, you must first globally enable QoS by entering the **mls qos** global configuration command.

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

http://www.cisco.com/en/US/products/ps6922/products_feature_guide09186a00807d72f5.html

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_configuration_guide_book09186a0080707055.html

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

http://www.cisco.com/en/US/products/ps6441/products_command_reference_book09186a008049739b.html

This section includes these procedures:

- [Manually Configuring an IP SLAs CFM Probe or Jitter Operation, page 41-10](#)
- [Configuring an IP SLAs Operation with Endpoint Discovery, page 41-12](#)

Manually Configuring an IP SLAs CFM Probe or Jitter Operation

Beginning in privileged EXEC mode, follow these steps to manually configure an IP SLAs Ethernet echo (ping) or jitter operation:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ip sla operation-number	Create an IP SLAs operation, and enter 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]	Configure the IP SLAs operation as an echo (ping) or jitter operation, and enter IP SLAs Ethernet echo configuration mode. <ul style="list-style-type: none"> • 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) Set 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) Set 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) Specify parameters for gathering statistical history information for the IP SLAs operation.

	Command	Purpose
Step 7	owner <i>owner-id</i>	(Optional) Configure the SNMP owner of the IP SLAs operation.
Step 8	request-data-size <i>bytes</i>	(Optional) Specify 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 <i>text</i>	(Optional) Create a user-specified identifier for an IP SLAs operation.
Step 10	threshold <i>milliseconds</i>	(Optional) Specify 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 <i>milliseconds</i>	(Optional) Specify 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	Return to global configuration mode.
Step 13	ip sla schedule <i>operation-number</i> [ageout <i>seconds</i>] [life { forever <i>seconds</i> }] [recurring] [start-time { <i>hh:mm:ss</i> <i>month day day month</i> } pending now after <i>hh:mm:ss</i>]	Schedule the time parameters for the IP SLAs operation. <ul style="list-style-type: none"> • <i>operation-number</i>—Enter the IP SLAs operation number. • (Optional) ageout <i>seconds</i>—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 <i>seconds</i>. 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: <ul style="list-style-type: none"> – 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 <i>hh:mm:ss</i> to show that the operation should start after the entered time has elapsed.
Step 14	end	Return to privileged EXEC mode.
Step 15	show ip sla configuration [<i>operation-number</i>]	Show the configured IP SLAs operation.
Step 16	copy running-config startup-config	(Optional) Save 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

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

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ip sla ethernet-monitor <i>operation-number</i>	Begin configuration of an IP SLAs automatic Ethernet operation, and enter IP SLAs Ethernet monitor configuration mode.
Step 3	type echo domain <i>domain-name</i> vlan <i>vlan-id</i> [exclude-mpids <i>mp-ids</i>] or type jitter domain <i>domain-name</i> vlan <i>vlan-id</i> [exclude-mpids <i>mp-ids</i>] [interval <i>interpacket-interval</i>] [num-frames <i>number-of-frames</i> <i>transmitted</i>]	Configure the automatic Ethernet operation to create echo (ping) or jitter operation and enter IP SLAs Ethernet echo configuration mode. <ul style="list-style-type: none"> • 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 <i>cos-value</i>	(Optional) Set 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	owner <i>owner-id</i>	(Optional) Configure the SNMP owner of the IP SLAs operation.
Step 6	request-data-size <i>bytes</i>	(Optional) Specify 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 <i>text</i>	(Optional) Create a user-specified identifier for an IP SLAs operation.
Step 8	threshold <i>milliseconds</i>	(Optional) Specify the upper threshold value in milliseconds for calculating network monitoring statistics. The range is 0 to 2147483647; the default is 5000.
Step 9	timeout <i>milliseconds</i>	(Optional) Specify 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.

	Command	Purpose
Step 10	exit	Return to global configuration mode.
Step 11	ip sla schedule <i>operation-number</i> [ageout <i>seconds</i>] [life { forever <i>seconds</i> }] [recurring] [start-time { <i>hh:mm:ss</i> [<i>month day</i> <i>day month</i>] pending now after <i>hh:mm:ss</i> }]	Schedule the time parameters for the IP SLAs operation. <ul style="list-style-type: none"> • <i>operation-number</i>—Enter the IP SLAs operation number. • (Optional) ageout <i>seconds</i>—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 <i>seconds</i>. 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: <ul style="list-style-type: none"> – 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 <i>hh:mm:ss</i> to show that the operation should start after the entered time has elapsed.
Step 12	end	Return to privileged EXEC mode.
Step 13	show ip sla configuration [<i>operation-number</i>]	Show the configured IP SLAs operation.
Step 14	copy running-config startup-config	(Optional) Save your entries in the configuration file.

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

Displaying Ethernet CFM Information

You can use the privileged EXEC commands in [Table 41-1](#) to display Ethernet CFM information.

Table 41-1 *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.

Table 41-1 Displaying CFM Information (continued)

Command	Purpose
<code>show ethernet cfm maintenance-points remote [detail domain level]</code>	Displays information about a remote maintenance point domains or levels or details in the CFM database.
<code>show ethernet cfm maintenance-points remote crosscheck</code>	Displays information about remote maintenance points configured statically in a crosscheck list.
<code>show ethernet cfm traceroute-cache</code>	Displays the contents of the traceroute cache.
<code>show platform cfm</code>	Displays platform-independent CFM information.

You can use the privileged EXEC commands in [Table 41-2](#) to display IP SLAs Ethernet CFM information.

Table 41-2 Displaying IP SLAs CFM Information

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

Understanding the Ethernet OAM Protocol

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, when you enable link monitoring, because the CPU must poll error counters frequently, 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. It 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 exceed 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 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.
- Remote loopback mode to ensure 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 in the up state. 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, page 41-16](#)
- [Ethernet OAM Configuration Guidelines, page 41-16](#)
- [Enabling Ethernet OAM on an Interface, page 41-16](#)
- [Enabling Ethernet OAM Remote Loopback, page 41-17](#)

- [Configuring Ethernet OAM Link Monitoring, page 41-18](#)
- [Configuring Ethernet OAM Remote Failure Indications, page 41-21](#)
- [Configuring Ethernet OAM Templates, page 41-21](#)

Default Ethernet OAM Configuration

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 supports generating 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.
- The switch does not support Ethernet OAM on ports that belong to an EtherChannel.

Enabling Ethernet OAM on an Interface

Beginning in privileged EXEC mode, follow these steps to enable Ethernet OAM on an interface:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>interface-id</i>	Define an interface to configure as an EOM interface, and enter interface configuration mode.
Step 3	ethernet oam	Enable Ethernet OAM on the interface.

	Command	Purpose
Step 4	ethernet oam [max-rate <i>oampdus</i> min-rate <i>seconds</i> mode { active passive } timeout <i>seconds</i>]	<p>You can configure these optional OAM parameters:</p> <ul style="list-style-type: none"> • (Optional) Enter max-rate <i>oampdus</i> to configure the maximum number of OAM PDUs sent per second. The range is from 1 to 10. • (Optional) Enter min-rate <i>seconds</i> 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. • (Optional) Enter mode passive to set OAM client mode to passive. <p>Note When Ethernet OAM mode is enabled on two interfaces passing traffic, at least one must be in the active mode.</p> <ul style="list-style-type: none"> • (Optional) Enter timeout <i>seconds</i> to set a time for OAM client timeout. The range is from 2 to 30.
Step 5	end	Return to privileged EXEC mode.
Step 6	show ethernet oam status [interface <i>interface-id</i>]	Verify the configuration.
Step 7	copy running-config startup-config	(Optional) Save your entries in the configuration file.

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

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:

- Internet Group Management Protocol (IGMP) packets are not looped back.
- You cannot configure Ethernet OAM remote loopback on ISL ports or ports that belong to an EtherChannel.
- If dynamic ARP inspection is enabled, ARP or reverse ARP packets are not looped or dropped.

Beginning in privileged EXEC mode, follow these steps to enable Ethernet OAM remote loopback on an interface:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>interface-id</i>	Define an interface to configure as an EOM interface, and enter interface configuration mode.

	Command	Purpose
Step 3	ethernet oam remote-loopback { supported timeout <i>seconds</i> }	Enable Ethernet remote loopback on the interface or set a loopback timeout period. <ul style="list-style-type: none"> Enter supported to enable remote loopback. Enter timeout <i>seconds</i> to set a remote loopback timeout period. The range is from 1 to 10 seconds.
Step 4	end	Return to privileged EXEC mode.
Step 5	ethernet oam remote-loopback { start stop } { interface <i>interface-id</i> }	Turn on or turn off Ethernet OAM remote loopback on an interface.
Step 6	show ethernet oam status [interface <i>interface-id</i>]	Verify the configuration.
Step 7	copy running-config startup-config	(Optional) Save 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.

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, it defaults to a value lower than the high threshold.

Beginning in privileged EXEC mode, follow these steps to configure Ethernet OAM link monitoring on an interface:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>interface-id</i>	Define an interface, and enter interface configuration mode.
Step 3	ethernet oam link-monitor supported	Enable 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.

	Command	Purpose
Step 4	<p>ethernet oam link-monitor symbol-period {threshold {high {high symbols none} low {low-symbols}} window symbols}</p> <p>Note Repeat this step to configure both high and low thresholds.</p>	<p>(Optional) Configure high and low thresholds for an error-symbol period that trigger an error-symbol period link event.</p> <ul style="list-style-type: none"> Enter threshold high <i>high-symbols</i> 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 <i>low-symbols</i> 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 <i>symbols</i> to set the window size (in number of symbols) of the polling period. The range is 1 to 65535 symbols.
Step 5	<p>ethernet oam link-monitor frame {threshold {high {high-frames none} low {low-frames}} window milliseconds}</p> <p>Note Repeat this step to configure both high and low thresholds.</p>	<p>(Optional) Configure high and low thresholds for error frames that trigger an error-frame link event.</p> <ul style="list-style-type: none"> Enter threshold high <i>high-frames</i> 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 <i>low-frames</i> to set a low threshold in number of frames. The range is 0 to 65535. The default is 1. Enter window <i>milliseconds</i> 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.
Step 6	<p>ethernet oam link-monitor frame-period {threshold {high {high-frames none} low {low-frames}} window frames}</p> <p>Note Repeat this step to configure both high and low thresholds.</p>	<p>(Optional) Configure high and low thresholds for the error-frame period that triggers an error-frame-period link event.</p> <ul style="list-style-type: none"> Enter threshold high <i>high-frames</i> 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 <i>low-frames</i> to set a low threshold in number of frames. The range is 0 to 65535. The default is 1. Enter window <i>frames</i> 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.

	Command	Purpose
Step 7	ethernet oam link-monitor frame-seconds { threshold { high { high-frames none } low { low-frames } } window milliseconds } Note Repeat this step to configure both high and low thresholds.	(Optional) Configure high and low thresholds for the frame-seconds error that triggers an error-frame-seconds link event. <ul style="list-style-type: none"> Enter threshold high <i>high-frames</i> 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 <i>low-frames</i> to set a low threshold in number of frames. The range is 1 to 900. The default is 1. Enter window <i>frames</i> 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.
Step 8	ethernet oam link-monitor receive-crc { threshold { high { high-frames none } low { low-frames } } window milliseconds } Note Repeat this step to configure both high and low thresholds.	(Optional) Configure thresholds for monitoring ingress frames received with cyclic redundancy code (CRC) errors for a period of time. <ul style="list-style-type: none"> Enter threshold high <i>high-frames</i> 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 <i>low-frames</i> to set a low threshold in number of frames. The range is 0 to 65535. The default is 1. Enter window <i>milliseconds</i> 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) Start 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	Return to privileged EXEC mode.
Step 11	show ethernet oam status [interface interface-id]	Verify the configuration.
Step 12	copy running-config startup-config	(Optional) Save 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 are allowed to enter it, but it is not supported. Enter the **no** form of the commands to disable the configuration. Use the **no** form of each command to disable the threshold setting.

Configuring Ethernet OAM Remote Failure Indications

You can configure an error-disable action to occur on an interface if one of the high thresholds is exceeded, if the remote link goes down, if the remote device is rebooted, or if the remote device disables Ethernet OAM on the interface.

Beginning in privileged EXEC mode, follow these steps to enable Ethernet OAM remote-failure indication actions on an interface:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>interface-id</i>	Define an interface, and enter interface configuration mode.
Step 3	ethernet oam remote-failure {critical-event dying-gasp link-fault} action error-disable-interface	Configure the Ethernet OAM remote-failure action on the interface. You can configure disabling the interface for one of these conditions: <ul style="list-style-type: none"> • Select critical-event to shut down the interface when an unspecified critical event has occurred. • Select dying-gasp to shut down the interface when Ethernet OAM is disabled or the interface enters the error-disabled state. • Select link-fault to shut down the interface when the receiver detects a loss of signal.
Step 4	end	Return to privileged EXEC mode.
Step 5	show ethernet oam status [interface interface-id]	Verify the configuration.
Step 6	copy running-config startup-config	(Optional) Save 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.

Beginning in privileged EXEC mode, follow these steps to configure an Ethernet OAM template and to associate it with an interface:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	template <i>template-name</i>	Create a template, and enter template configuration mode.
Step 3	ethernet oam link-monitor receive-crc { threshold { high { <i>high-frames</i> none } low { <i>low-frames</i> } } window <i>milliseconds</i> }	<p>(Optional) Configure thresholds for monitoring ingress frames received with cyclic redundancy code (CRC) errors for a period of time.</p> <ul style="list-style-type: none"> • Enter threshold high <i>high-frames</i> 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 <i>low-frames</i> to set a low threshold in number of frames. The range is 0 to 65535. The default is 1. • Enter window <i>milliseconds</i> 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 { <i>high symbols</i> none } low { <i>low-symbols</i> } } window <i>symbols</i> }	<p>(Optional) Configure high and low thresholds for an error-symbol period that triggers an error-symbol period link event.</p> <ul style="list-style-type: none"> • Enter threshold high <i>high-symbols</i> 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 <i>low-symbols</i> 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 <i>symbols</i> 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 { <i>high-frames</i> none } low { <i>low-frames</i> } } window <i>milliseconds</i> }	(Optional) Configure high and low thresholds for error frames that trigger an error-frame link event. <ul style="list-style-type: none"> • Enter threshold high <i>high-frames</i> 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 <i>low-frames</i> to set a low threshold in number of frames. The range is 0 to 65535. The default is 1. • Enter window <i>milliseconds</i> 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 { <i>high-frames</i> none } low { <i>low-frames</i> } } window <i>frames</i> }	(Optional) Configure high and low thresholds for the error-frame period that triggers an error-frame-period link event. <ul style="list-style-type: none"> • Enter threshold high <i>high-frames</i> 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 <i>low-frames</i> to set a low threshold in number of frames. The range is 0 to 65535. The default is 1. • Enter window <i>frames</i> 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 { <i>high-seconds</i> none } low { <i>low-seconds</i> } } window <i>milliseconds</i> }	(Optional) Configure frame-seconds high and low thresholds for triggering an error-frame-seconds link event. <ul style="list-style-type: none"> • Enter threshold high <i>high-seconds</i> 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 <i>low-frames</i> to set a low threshold in number of frames. The range is 1 to 900. The default is 1. • Enter window <i>frames</i> 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) Configure the switch to put an interface in an error disabled state when a high threshold for an error is exceeded.
Step 9	exit	Return to global configuration mode.
Step 10	interface <i>interface-id</i>	Define an Ethernet OAM interface, and enter interface configuration mode.
Step 11	source-template <i>template-name</i>	Associate the template to apply the configured options to the interface.
Step 12	end	Return to privileged EXEC mode.
Step 13	show ethernet oam status [interface <i>interface-id</i>]	Verify the configuration.
Step 14	copy running-config startup-config	(Optional) Save 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* to remove the source template association.

Displaying Ethernet OAM Protocol Information

You can use the privileged EXEC commands in [Table 41-3](#) to display Ethernet OAM protocol information.

Table 41-3 *Displaying Ethernet OAM Protocol Information*

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

Understanding E-LMI

Ethernet Local Management Interface (E-LMI) is a protocol between the customer-edge (CE) device and the provider-edge (PE) device. It runs only on the PE-to-CE UNI link and notifies the CE device of connectivity status and configuration parameters of Ethernet services available on the CE port. E-LMI interoperates with an OAM protocol, such as CFM, that runs within the provider network to collect OAM status. CFM runs at the provider maintenance level (UPE to UPE with inward-facing MEPs at the UNI). E-LMI relies on the OAM Ethernet Infrastructure to interwork with CFM for end-to-end status of Ethernet virtual connections (EVCs) across CFM domains.

OAM manager, which streamlines interaction between any two OAM protocols, handles the interaction between CFM and E-LMI. This interaction is unidirectional, running only from OAM manager to E-LMI on the UPE side of the switch. Information is exchanged either as a result of a request from E-LMI or triggered by OAM when it received notification of a change from the OAM protocol. This type of information is relayed:

- EVC name and availability status
- Remote UNI name and status
- Remote UNI counts

You can configure Ethernet virtual connections (EVCs), service VLANs, UNI ids (for each CE-to-PE link), and UNI count and attributes. You need to configure CFM to notify the OAM manager of any change to the number of active UNIs and or the remote UNI ID for a given S-VLAN domain.

You can configure the switch as either the customer-edge device or the provider-edge device.

E-LMI Interaction with OAM Manager

No interactions are required between E-LMI and OAM manager on the CE side. On the UPE side, OAM manager defines an abstraction layer that relays data collected from OAM protocols (in this case CFM) running within the metro network to the E-LMI switch. The information flow is unidirectional (from OAM manager to the E-LMI) but is triggered in one of two ways:

- Synchronous data flow triggered by a request from the E-LMI
- Asynchronous data flow triggered by OAM manager when it receives notification from CFM that the number of remote UNIs has changed

This data includes:

- EVC name and availability status (active, not active, partially active, or not defined)
- Remote UNI name and status (up, disconnected, administratively down, excessive FCS failures, or not reachable)
- Remote UNI counts (the total number of expected UNIs and the actual number of active UNIs)

The asynchronous update is triggered only when the number of active UNIs has changed.

CFM Interaction with OAM Manager

When there is a change in the number of active UNIs or remote UNI ID for a given S-VLAN or domain, CFM asynchronously notifies the OAM manager. A change in the number of UNIs might (or might not) cause a change in EVC status. OAM manager calculates EVC status given the number of active UNIs and the total number of associated UNIs.

**Note**

If crosscheck is disabled, no SNMP traps are sent when there is a change in the number of UNIs.

Configuring E-LMI

For E-LMI to work with CFM, you configure Ethernet virtual connections (EVCs), Ethernet service instances (EFPs), and E-LMI customer VLAN mapping. Most of the configuration occurs on the PE switch on the interfaces connected to the CE device. On the CE switch, you only need to enable E-LMI on the connecting interface. Note that you must configure some OAM parameters, for example, EVC definitions, on PE devices on both sides of a metro network.

This section includes this information:

- [Default E-LMI Configuration, page 41-26](#)
- [E-LMI and OAM Manager Configuration Guidelines, page 41-26](#)
- [Configuring the OAM Manager, page 41-27](#)
- [Enabling E-LMI, page 41-29](#)
- [Ethernet OAM Manager Configuration Example, page 41-30](#)

Default E-LMI Configuration

Ethernet LMI is globally disabled by default. When enabled, the switch is in provider-edge (PE) mode by default.

When you globally enable E-LMI by entering the **ethernet lmi global** global configuration command, it is automatically enabled on all interfaces. You can also enable or disable E-LMI per interface to override the global configuration. The E-LMI command that is given last is the command that has precedence.

There are no EVCs, EFP service instances, or UNIs defined.

UNI bundling service is bundling with multiplexing.

E-LMI and OAM Manager Configuration Guidelines

OAM manager is an infrastructural element and requires two interworking OAM protocols, in this case CFM and E-LMI. For OAM to operate, the PE side of the connection must be running CFM and E-LMI.

- E-LMI is not supported on routed ports, EtherChannel port channels or ports that belong to an EtherChannel, private VLAN ports, IEEE 802.1Q tunnel ports, or EoMPLS ports.
- You cannot configure E-LMI on VLAN interfaces.
- When you enable E-LMI globally or on an interface, the switch is in PE mode by default. You must enter the **ethernet lmi ce** global configuration command to enable the switch or interface in customer-edge mode.
- When the switch is configured as a CE device, the **service instance** and **ethernet uni** interface commands are visible but not supported.

Configuring the OAM Manager

Beginning in privileged EXEC mode, follow these steps to configure OAM manager on a PE switch:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ethernet cfm domain <i>domain-name</i> level <i>level-id</i>	Define 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.
Step 3	service <i>csi-id</i> vlan <i>vlan-id</i>	Define a universally unique customer service instance (CSI) and VLAN ID within the maintenance domain. <ul style="list-style-type: none"> <i>csi-id</i>—a string of no more than 100 characters that identifies the CSI. <i>vlan-id</i>—VLAN range is from 1 to 4095. You cannot use the same VLAN ID for more than one domain at the same level.
Step 4	exit	Return to global configuration mode.
Step 5	ethernet evc <i>evc-id</i>	Define an Ethernet virtual connection (evc), and enter evc configuration mode. The identifier can be up to 100 characters in length.
Step 6	oam protocol cfm svlan <i>vlan-id</i> domain <i>domain-name</i>	Configure the EVC OAM protocol as CFM, and identify the service provider VLAN-ID (S-VLAN-ID) for the CFM domain maintenance level as configured in Steps 2 and 3. <p>Note If the CFM domain does not exist, the command is rejected, and an error message appears.</p>
Step 7	uni count <i>value</i>	(Optional) Set the UNI count for the EVC. The range is 2 to 1024; the default is 2. <p>If the command is not entered, the service defaults to a point-to-point service. If you enter a value of 2, you have the option to select point-to-multipoint service. If you configure a value of 3 or greater, the service is point-to-multipoint.</p> <p>Note You should know the correct number of maintenance end points in the domain. If you enter a value greater than the actual number of end points, the UNI status will show as partially active even if all end points are up; if you enter a uni count less than the actual number of end points, status might show as active, even if all end points are not up.</p>
Step 8	exit	Return to global configuration mode.
Step 9	Repeat Steps 2 to 5 for other CFM domains that you want OAM manager to monitor.	
Step 10	interface <i>interface-id</i>	Specify a physical interface connected to the CE device, and enter interface configuration mode.

	Command	Purpose
Step 11	<code>service instance <i>efp-identifier</i> ethernet [<i>evc-id</i>]</code>	Configure an Ethernet service instance (EFP) on the interface, and enter ethernet service configuration mode. <ul style="list-style-type: none"> The EFP identifier is a per-interface service identifier that does not map to a VLAN. The EFP identifier range is 1 to 4967295. (Optional) Enter an <i>evc-id</i> to attach an EVC to the EFP.
Step 12	<code>ethernet lmi ce-vlan map {<i>vlan-id</i> any default untagged}</code>	Configure an E-LMI customer VLAN-to-EVC map for a particular UNI. The keywords have these meanings: <ul style="list-style-type: none"> For vlan <i>vlan-id</i>, enter the customer VLAN ID or IDs to map to as single VLAN-ID (1 to 4094), a range of VLAN-IDs separated by a hyphen, or a series of VLAN IDs separated by commas. Enter any to map all VLANs (untagged or 1 to 4094). Enter default to map the default EFP. You can use default keyword only if you have already mapped the service instance to a VLAN or group of VLANs. Enter untagged to map untagged VLANs.
Step 13	<code>exit</code>	Return to interface configuration mode.
Step 14	<code>ethernet uni id <i>name</i></code>	Configure an Ethernet UNI ID. The name should be unique for all the UNIs that are part of a given customer service instance and can be up to 64 characters in length. When a UNI id is configured on a port, that ID is used as the default name for all MEPs configured on the port, unless a name is explicitly configured for a given MEP. <p>Note This command is required on all ports that are directly connected to CE devices. If the specified ID is not unique on the device, an error message appears.</p>
Step 15	<code>ethernet uni { bundle [all-to-one] multiplex}</code>	(Optional) Set UNI bundling attributes: <ul style="list-style-type: none"> If you enter bundle <cr>, the UNI supports bundling without multiplexing (only one EVC with one or multiple VLANs be mapped to it). If you enter bundle all-to-one, the UNI supports a single EVC and all VLANs are mapped to that EVC. If you enter multiplex, the UNI supports multiplexing without bundling (one or more EVCs with a single VLAN mapped to each EVC). <p>If you do not configure bundling attributes, the default is bundling with multiplexing (one or more EVCs with one or more VLANs mapped to each EVC).</p>
Step 16	<code>end</code>	Return to privileged EXEC mode.
Step 17	<code>show ethernet service evc {detail id <i>evc-id</i> interface <i>interface-id</i>}</code>	Verify the configuration.
Step 18	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

Use the **no** forms of the commands to delete an EVC, EFP, or UNI ID, or to return to default configurations.

**Note**

If you configure, change, or remove a UNI service type, EVC, EFP, or CE-VLAN configuration, all configurations are checked to make sure that the configurations match (UNI service type with EVC or EFP and CE-VLAN configuration). The configuration is rejected if the configurations do not match.

Enabling E-LMI

You can enable E-LMI globally or on an interface and you can configure the switch as a PE or a CE device. Beginning in privileged EXEC mode, follow these steps to enable for E-LMI on the switch or on an interface. Note that the order of the global and interface commands determines the configuration. The command that is entered last has precedence.

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ethernet lmi global	Globally enable E-LMI on all interfaces. By default, the switch is a PE device.
Step 3	ethernet lmi ce	(Optional) Configure the switch as an E-LMI CE device.
Step 4	interface <i>interface-id</i>	Define an interface to configure as an E-LMI interface, and enter interface configuration mode.
Step 5	ethernet lmi interface	Configure Ethernet LMI on the interface. If E-LMI is enabled globally, it is enabled on all interfaces unless you disable it on specific interfaces. If E-LMI is disabled globally, you can use this command to enable it on specified interfaces.

	Command	Purpose
Step 6	<code>ethernet lmi {n391 value n393 value t391 value t392 value}</code>	<p>Configure E-LMI parameters for the UNI.</p> <p>The keywords have these meanings:</p> <ul style="list-style-type: none"> • n391 value—Set the event counter on the customer equipment. The counter polls the status of the UNI and all Ethernet virtual connections (EVCs). The range is from 1 to 65000; the default is 360. • n393 value—Set the event counter for the metro Ethernet network. The range is from 1 to 10; the default is 4. • t391 value—Set the polling timer on the customer equipment. A polling timer sends status enquiries and when status messages are not received, records errors. The range is from 5 to 30 seconds; the default is 10 seconds. • t392 value—Set the polling verification timer for the metro Ethernet network or the timer to verify received status inquiries. The range is from 5 to 30 seconds, or enter 0 to disable the timer. The default is 15 seconds. <p>Note The t392 keyword is not supported when the switch is in CE mode.</p>
Step 7	<code>end</code>	Return to privileged EXEC mode.
Step 8	<code>show ethernet lmi evc</code>	Verify the configuration.
Step 9	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

Use the **no ethernet lmi** global configuration command to globally disable E-LMI. Use the **no** form of the **ethernet lmi** interface configuration command with keywords to disable E-LMI on the interface or to return the timers to the default settings.

Use the **show ethernet lmi** commands to display information that was sent to the CE from the status request poll. Use the **show ethernet service** commands to show current status on the device.

Ethernet OAM Manager Configuration Example

This is a simple example of configuring CFM and E-LMI with OAM manager on a PE device and on a CE device. You can configure the switch as either the PE device or the CE device.

Provider-Edge Device Configuration

This example shows a sample configuration of OAM manager, CFM, and E-LMI on the PE device:

```
Switch# config t
Switch(config)# ethernet cfm domain Top level 7
Switch(config)# ethernet cfm domain Provider level 4
Switch(config-ether-cfm)# service customer_1 vlan 101
Switch(config-ether-cfm)# mep crosscheck mpid 404 vlan 101
Switch(config-ether-cfm)# exit
Switch(config)# ethernet cfm domain Operator_level 2
Switch(config-ether-cfm)# service operator_1 vlan 101
```

```

Switch(config-ether-cfm)# exit
Switch(config)# ethernet cfm enable
Switch(config)# ethernet evc test1
Switch(config-enc)# oam protocol cfm svlan 101 domain Provider
Switch(config-enc)# exit
Switch(config)# ethernet evc 101
Switch(config-enc)# uni count 3
Switch(config-enc)# oam protocol cfm svlan 101 domain Operator
Switch(config-enc)# exit
Switch(config)# ethernet lmi global
Switch(config)# interface gigabitethernet 1/0/2
Switch(config-if)# ethernet cfm mip level 7
Switch(config-if)# ethernet cfm mep level 4 mpid 200 vlan 200
Switch(config-if)# service instance 101 ethernet test1
Switch(config-if-srv)# ethernet lmi ce-vlan map 101
Switch(config-if-srv)# exit
Switch(config-if)# exit
Switch(config)# ethernet cfm cc enable level 2-4 vlan 101
Switch(config)# exit

```

Customer-Edge Device Configuration

This example shows the commands necessary to configure E-LMI on the CE device. Beginning with Cisco IOS Release 12.2(37)SE, the switch can be configured as the CE device.

This example enables E-LMI globally, but you can also enable it only on a specific interface. However, if you do not enter the **ethernet lmi ce** global configuration command, the interface will be in PE mode by default.

```

Switch# config t
Switch(config)# ethernet lmi global
Switch(config)# ethernet lmi ce
Switch(config)# exit

```



Note

For E-LMI to work, any VLANs used on the PE device must also be created on the CE device. Create a VLAN by entering the **vlan *vlan-id*** global configuration command on the CE device, where the *vlan-ids* match those on the PE device and configure these VLANs as allowed VLANs by entering the **switchport trunk allowed vlan *vlan-ids*** interface configuration command. Allowed VLANs can receive and send traffic on the interface in tagged format when in trunking mode.

Displaying E-LMI and OAM Manager Information

You can use the privileged EXEC commands in [Table 41-4](#) to display E-LMI or OAM manager information.

Table 41-4 Displaying E-LMI and OAM Manager Information

Command	Purpose
show ethernet lmi evc [detail <i>evc-id</i> [interface <i>interface-id</i>] map interface <i>type number</i>]	Displays details sent to the CE from the status request poll about the E-LMI EVC.
show ethernet lmi parameters interface <i>interface-id</i>	Displays Ethernet LMI interface parameters sent to the CE from the status request poll.

Table 41-4 Displaying E-LMI and OAM Manager Information (continued)

Command	Purpose
show ethernet lmi statistics interface <i>interface-id</i>	Displays Ethernet LMI interface statistics sent to the CE from the status request poll.
show ethernet lmi uni map interface [<i>interface-id</i>]	Displays information about the E-LMI UNI VLAN map sent to the CE from the status request poll.
show ethernet service evc { detail id <i>evc-id</i> interface <i>interface-id</i> }	Displays information about the specified Ethernet virtual connection (EVC) customer-service instance or all configured service instances.
show ethernet service instance { detail id <i>efp-identifier</i> interface <i>interface-id</i> interface <i>interface-id</i> }	Displays information relevant to the specified Ethernet service instances (EFPs).
show ethernet service interface [<i>interface-id</i>] [detail]	Displays information about OAM manager interfaces.

Ethernet CFM and Ethernet OAM Interaction

Beginning with Cisco IOS Release 12.2(40)SE, you can also configure the OAM Manager infrastructure for interaction 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 OAMPDU 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.

This section includes this information:

- [Configuring Ethernet OAM Interaction with CFM, page 41-33](#)
- [Ethernet OAM and CFM Configuration Example, page 41-34](#)

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/products/ps6922/products_feature_guide09186a008066fcb8.html

Configuring Ethernet OAM Interaction with CFM

For Ethernet OAM to function with CFM, you must configure an Ethernet Virtual Circuit (EVC) and the OAM manager, and associate the EVC with CFM. You must use an inward facing MEP for interaction with the OAM manager.



Note

If you configure, change, or remove a UNI service type, EVC, Ethernet service instance, or CE-VLAN configuration, all configurations are verified to ensure that the UNI service types match the EVC configuration and that Ethernet service instances are matched with the CE-VLAN configuration. Configurations are rejected if the pairs do not match.

Configuring the OAM Manager

Beginning in privileged EXEC mode, follow these steps to configure the OAM manager on a PE device:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ethernet cfm domain <i>domain-name</i> level <i>level-id</i>	Define 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.
Step 3	service <i>csi-id</i> vlan <i>vlan-id</i>	Define a universally unique customer service instance (CSI) and VLAN ID within the maintenance domain. <ul style="list-style-type: none"> • <i>csi-id</i>—String of no more than 100 characters that identifies the CSI. • <i>vlan-id</i>—VLAN range is from 1 to 4095. You cannot use the same VLAN ID for more than one domain at the same level.
Step 4	exit	Return to global configuration mode.
Step 5	ethernet evc <i>evc-id</i>	Define an EVC, and enter EVC configuration mode
Step 6	oam protocol cfm svlan <i>vlan-id</i> domain <i>domain-name</i>	Configure the EVC OAM protocol as CFM, and identify the service provider VLAN-ID (S-VLAN-ID) for the CFM domain maintenance level as configured in Steps 2 and 3.
Step 7	exit	Return to global configuration mode.
Step 8	Repeat Steps 2 through 7 to define other CFM domains that you want OAM manager to monitor.	
Step 9	ethernet cfm enable	Globally enable CFM.
Step 10	end	Return to privileged EXEC mode.
Step 11	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Enabling Ethernet OAM

Beginning in privileged EXEC mode, follow these steps to enable Ethernet OAM on an interface.

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>interface interface-id</code>	Define an interface to configure as an Ethernet OAM interface and enter interface configuration mode.
Step 3	<code>ethernet oam [max-rate oampdus min-rate seconds mode {active passive} timeout seconds]</code>	Enable Ethernet OAM on the interface <ul style="list-style-type: none"> • (Optional) Enter max-rate oampdus to set the maximum rate (per second) to send OAM PDUs. The range is 1 to 10 PDUs per second; the default is 10. • (Optional) Enter min-rate seconds to set the minimum rate in seconds. The range is 1 to 10 seconds. • (Optional) Set the OAM client mode as active or passive. The default is active. • (Optional) Enter timeout seconds to set the time after which a device declares the OAM peer to be nonoperational and resets its state machine. The range is 2 to 30 seconds; the default is 5 seconds.
Step 4	<code>end</code>	Return to privileged EXEC mode.
Step 5	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.
Step 6	<code>show ethernet cfm maintenance points remote</code>	(Optional) Display the port states as reported by Ethernet OAM.

Ethernet OAM and CFM Configuration Example

These are example configurations of the interworking between Ethernet OAM and CFM in a sample service provider network with 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 gigabitethernet1/0/1
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 fastethernet1/0/20
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 10
Switch(config-if)# ethernet uni id 2004-20
```

```
Switch(config-if)# ethernet oam remote-loopback supported
Switch(config-if)# ethernet oam
Switch(config-if)# service instance 10 ethernet BLUE
Switch(config-if-srv)# ethernet lmi ce-vlan map 10
Switch(config-if-srv)# exit
```

Provider-edge switch 2 (PE2) configuration:

```
Switch# config t
Switch(config)# interface gigabitEthernet1/1/20
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 uni id 2004-20
Switch(config-if)# ethernet oam remote-loopback supported
Switch(config-if)# ethernet oam
Switch(config-if)# service instance 10 ethernet BLUE
Switch(config-if-srv)# ethernet lmi ce-vlan map 10
Switch(config-if-srv)# exit
```

Customer-edge switch 2 (CE2) configuration:

```
Switch# config t
Switch(config)# interface gigabitEthernet1/0/1
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 are examples of the output showing 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           Gi1/1/1          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           Gi1/1/1          8       blue
Total Remote MEPs: 1
```

This example shows the outputs 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 goes into error-disable mode.

```
Switch# ethernet oam remote-loopback start interface gigabitEthernet 0/1
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           Gi1/1/1          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      Gi1/1/1          8         blue
Total Remote MEPS: 1
```

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