Configuring Ethernet CFM and E-LMI

Metro Ethernet service providers in particular require certain management capability within the context of the overall Ethernet infrastructure (EI). Ethernet operation, administration, and maintenance (OAM) refers to a set of tools and protocols used to install, monitor, and troubleshoot a network. Two of these functions are now supported by the Catalyst 3750 Metro switch.

This chapter provides general information about configuring IEEE 802.1ag Connectivity Fault Management (CFM) and Ethernet Local Management Interface (E-LMI). Ethernet OAM manager is the facility that handles the interworking between CFM and E-LMI.

For complete command and configuration information for CFM, see the 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.

This chapter consists of these sections:

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 (PE) to PE device or customer edge (CE) to CE device. Ethernet CFM, as specified by the IEEE 802.1ag, is the standard for Layer 2 ping, Layer 2 traceroute, and end-to-end connectivity check of the Ethernet network.

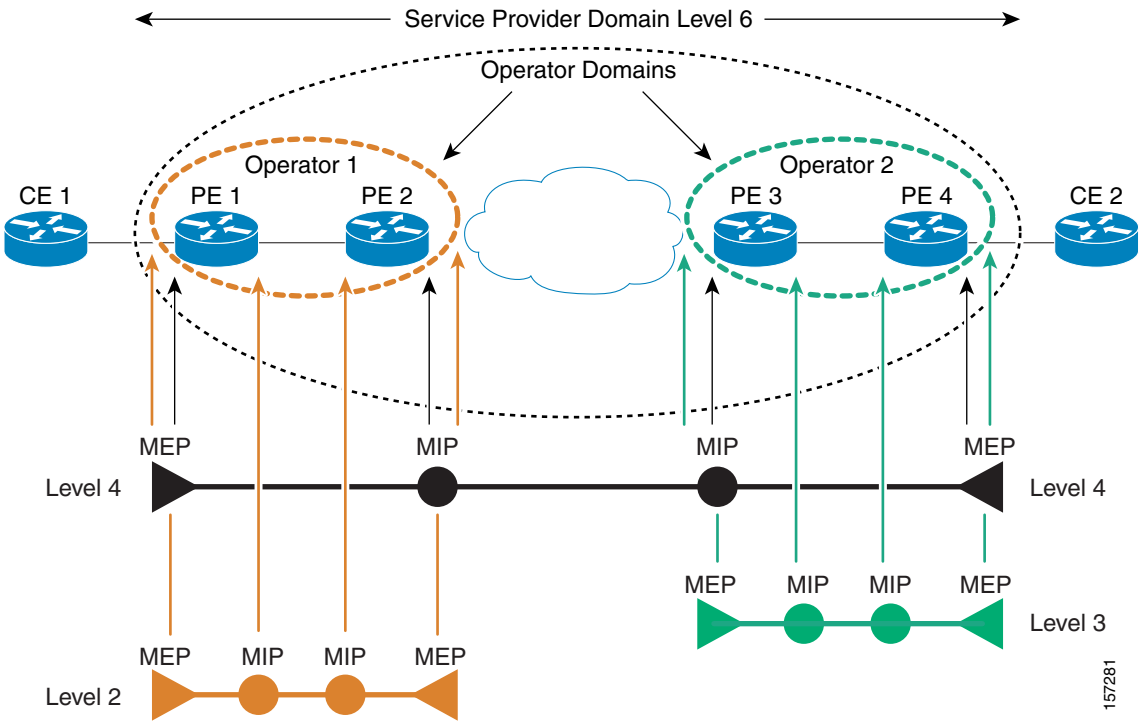
Note You configure E-LMI between the user provider edge (UPE) and the CE device, and it relies on CFM for reporting status of the metro Ethernet network to the CE.

These sections contain this conceptual information about Ethernet CFM:

CFM Domain

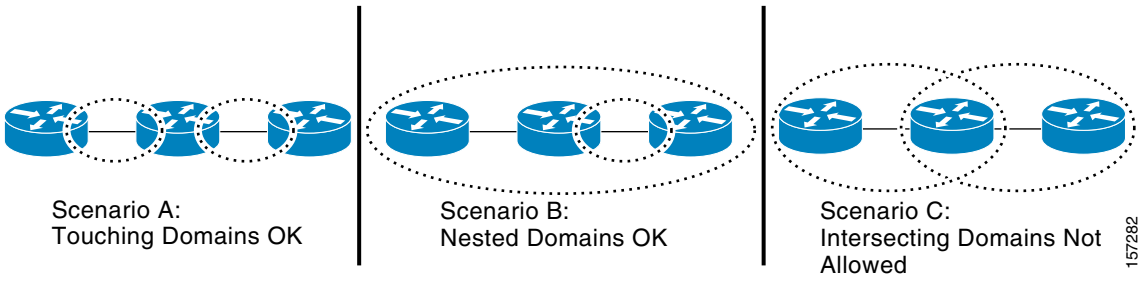
A CFM maintenance domain is a management space on a network that is owned and operated by a single entity and defined by a set of ports internal to it, but at its boundary. The network administrator assigns a unique maintenance level (from 0 to 7) to define the hierarchical relationship between domains. The larger the domain, the higher the level. For example, as shown in Figure 36-1, 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.

Figure 36-1 CFM Maintenance Domains



As shown in Figure 36-2, 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 36-2 Allowed Domain Relationships



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 CC 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 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.

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

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 a 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, EtherChannel port channels or ports that belong to an EtherChannel.
- You cannot configure CFM on VLAN interfaces.
- You cannot configure CFM on an EoMPLS port.
- CFM is not supported on private VLAN ports or IEEE 802.1Q tunnel ports. The configuration is allowed, but does not take affect.

Preparing the Ethernet CFM Network

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

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ethernet cfm traceroute cache** [**size** *entries* | **hold-time** *minutes*]	(Optional) Configure 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 3	**ethernet cfm domain** *domain-name* **level** *level-id*	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	**mep archive-hold-time** *minutes*	(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	**exit**	Return to global configuration mode.
Step 6	**interface** *interface-id*	Specify a physical interface to configure, and enter interface configuration mode.
Step 7	**ethernet cfm mip level** *level-id*	Configure 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 8	**exit**	Return to global configuration mode.
Step 9	**ethernet cfm cc** {[**enable**] **level** {*level-id* | **any**} **vlan** {*vlan-id* | **any**}}	Configure 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 10	**end**	Return to privileged EXEC mode.
Step 11	**show ethernet cfm domain brief** **show ethernet cfm maintenance-points local** **show ethernet cfm traceroute-cache**	Verify the configuration

	Command	Purpose
Step 12	**show running-config**	Verify your entries.
Step 13	**copy running-config startup-config**	(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	**configure terminal**	Enter global configuration mode.
Step 2	**ethernet cfm domain** *domain-name* **level** *level-id*	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** *csi-id* **vlan** *vlan-id*	Define a universally unique customer service instance (CSI) and VLAN ID within the maintenance domain. • *csi-id*—a string of no more than 100 characters that identifies the CSI. • *vlan-id*—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 cfm enable**	Globally enable CFM.
Step 6	**interface** *interface-id*	Specify a physical interface to configure, and enter interface configuration mode.
Step 7	**ethernet cfm mip level** *level-id*	Configure a customer level or service-provider level maintenance intermediate point (MIP) for the interface. The MIP level range is 0 to 7. **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 8	**ethernet cfm mep level** *level-id* [**inward**] **mpid** *identifier* **vlan** *vlan-id*	Configure maintenance end points (MEPs). for different maintenance levels. The MEP level range is 0 to 7. • (Optional) Specify the end point in the **inward** direction. • For **mpid** *identifier*, enter a maintenance end point identifier. 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.

	Command	Purpose
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** *delay*	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** *domain-name* **level** *level-id*	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	**mep crosscheck mpid** *identifier* **vlan** *vlan-id* [**mac** *remote MAC address*]	Define a remote maintenance end point (MEP) within a maintenance domain. • For **mpid** *identifier*, enter a maintenance end point identifier. The range is 1 to 8191. • For **vlan** *vlan-id*, 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** *level-id* **vlan** {*vlan-id* | **any**}	Enable or disable 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 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.

	Command	Purpose
Step 8	**show ethernet cfm maintenance-points remote crosscheck**	Verify the configuration
Step 9	**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.

Displaying Ethernet CFM Information

You can use the privileged EXEC commands in Table 36-1 to display Ethernet CFM information.

Table 36-1 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.
show ethernet cfm maintenance-points local	Displays maintenance points configured on a device.
show ethernet cfm maintenance-points remote [detail | domain | level]	Displays display information about a remote maintenance point domains or levels or details in the cc 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.
show platform cfm	Displays platform-independent CFM information.

Understanding E-LMI and Interactions with CFM

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-CE UNI link and notifies the CE 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 (EI) to interwork with CFM for end-to-end status of Ethernet virtual connections (EVCs) across CFM domains.

OAM manager streamlines interaction between OAM protocols, and handles the interaction between CFM and E-LMI. E-LMI interaction with OAM manager 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.

E-LMI implementation on the Catalyst 3750 Metro switch includes only PE-side support.

E-LMI Interaction with OAM Manager

No interactions are required between E-LMI and OAM manager on the CE (customer edge) side. On the UPE side, the 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 the 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. If only the UNI ID changes, a configuration change notification is sent from OAM manager to the E-LMI.

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 to Interaction with CFM

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. 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.

Default E-LMI and OAM Configuration

Ethernet LMI is globally disabled 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 command 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.

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.

Configuring 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** *domain-name* **level** *level-id*	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** *csi-id* **vlan** *vlan-id*	Define a universally unique customer service instance (CSI) and VLAN ID within the maintenance domain. • *csi-id*—a string of no more than 100 characters that identifies the CSI. • *vlan-id*—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** *evc-id*	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** *vlan-id* **domain** *domain-name*	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. **Note** If the CFM domain does not exist, the command is rejected, and an error message appears.

	Command	Purpose
Step 7	**uni count** *value*	(Optional) Set the UNI count for the EVC. The range is 2 to 1024; the default is 2. 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. **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 will show as active, even if all end points are not up.
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** *interface-id*	Specify a physical interface connected to the CE device, and enter interface configuration mode.
Step 11	**service instance** *efp-identifier* **ethernet** [*evc-id*]	Configure an Ethernet service instance (EFP) on the interface, and enter ethernet service configuration mode. • 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 *evc-id* to attach an EVC to the EFP.
Step 12	**ethernet lmi ce-vlan map** {*vlan-id* | **any** | **default** | **untagged**}	Configure an E-LMI customer VLAN-to-EVC map for a particular UNI. The keywords have these meanings: • For **vlan** *vlan-id*, 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	**exit**	Return to interface configuration mode.

	Command	Purpose
Step 14	**ethernet uni id** *name*	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. **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.
Step 15	**ethernet uni** {**bundle** [**all-to-one**] | **multiplex**}	(Optional) Set UNI bundling attributes: • 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). 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).
Step 16	**end**	Return to privileged EXEC mode.
Step 17	**show ethernet service evc** {**detail** | **id** *evc-id* | **interface** *interface-id*}	Verify the configuration
Step 18	**copy running-config startup-config**	(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

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.

	Command	Purpose
Step 3	**interface** *interface-id*	Define an interface to configure as an E-LMI interface, and enter interface configuration mode.
Step 4	**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.
Step 5	**ethernet lmi** {**n393** *value* | **t392** *value*}	Configure E-LMI parameters for the UNI. The keywords have these meanings: • **n393** *value*—Set the event counter for the metro Ethernet network. The range is from 1 to 10; the default is 4. • **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.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show ethernet lmi evc**	Verify the configuration
Step 8	**copy running-config startup-config**	(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.

Displaying E-LMI and OAM Manager Information

You can use the privileged EXEC commands in Table 36-2 to display E-LMI or OAM manager information.

Table 36-2 Displaying E-LMI and OAM Manager Information

Command	Purpose
show ethernet lmi evc	Displays brief details about the E-LMI EVC.
show ethernet lmi parameters	Displays Ethernet LMI parameters.
show ethernet lmi statistics	Displays Ethernet LMI statistics.
show ethernet lmi uni map	Displays information about the E-LMI UNI.
show ethernet service evc {**detail** | **id** *evc-id* | **interface** *interface-id*}	Displays information about the specified customer service instance or all configured service instances.
show ethernet service instance {**detail** | **id** *efp-identifier* **interface** *interface-id* | **interface** *interface-id*}	Displays information relevant to the specified EFP.
show ethernet service interface [*interface-id*] [**detail**]	Displays information about OAM manager interfaces.

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.

PE 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-evc)# oam protocol cfm svlan 101 domain Provider
Switch(config-evc)# exit
Switch(config)# ethernet evc 101
Switch(config-evc)# uni count 3
Switch(config-evc)# oam protocol cfm svlan 101 domain Operator
Switch(config-evc)# exit
Switch(config)# ethernet lmi global
Switch(config)# interface gigabitethernet 1/0/2
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
```

CE Configuration

This example shows the only command necessary to configure E-LMI on the CE device. The command globally enables E-LMI, but you can also enable it only on a specific interface.

```
Switch# config t
Switch(config)# ethernet lmi global
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.