CHAPTER 34

Configuring Ethernet OAM (IEEE 802.3ah), CFM (IEEE 802.1ag), and E-LMI on the ML-MR-10 Card

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 ML-MR-10 card 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. 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 on the ML-MR-10 card.

This chapter contains these sections:

Ethernet Connectivity Fault Management

Ethernet CFM is an end-to-end per-service-instance EOAM protocol. It includes proactive connectivity monitoring, fault verification, and fault isolation for large Ethernet metropolitan-area networks (MANs) and WANs.

The advent of Ethernet as a MAN and WAN technology imposes a new set of OAM requirements on Ethernet's traditional operations, which were centered on enterprise networks only. The expansion of Ethernet technology into the domain of service providers, where networks are substantially larger and more complex than enterprise networks and the user base is wider, makes operational management of link uptime crucial. More importantly, the timeliness in isolating and responding to a failure becomes mandatory for normal day-to-day operations, and OAM translates directly to the competitiveness of the service provider.

Troubleshooting carrier networks offering Ethernet Layer 2 services is challenging. Customers contract with service providers for end-to-end Ethernet service and service providers may subcontract with operators to provide equipment and networks. Compared to enterprise networks, where Ethernet traditionally has been implemented, these constituent networks belong to distinct organizations or departments, are substantially larger and more complex, and have a wider user base. Ethernet CFM provides a competitive advantage to service providers for which the operational management of link uptime and timeliness in isolating and responding to failures is crucial to daily operations.

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 customer-edge (CE) device and relies on CFM for reporting status of the metro-Ethernet network to the customer-edge device.

Understanding Ethernet CFM

Before you set up Ethernet CFM, you should understand the following concepts:

- Ethernet CFM Support on the ML-MR-10 Card, page 34-2
- View of CFM Interaction on different Networks with ML-MR-10 Card, page 34-10
- Customer Service Instance, page 34-4
- Maintenance Domain, page 34-5
- Maintenance Point, page 34-6
- CFM Messages, page 34-8
- View of CFM Interaction on different Networks with ML-MR-10 Card, page 34-10

Ethernet CFM Support on the ML-MR-10 Card

Ethernet CFM on the ML-MR-10 card provides the following support:

- End-to-end service-level OAM technology
- Reduced operating expense for service provider Ethernet networks
- Competitive advantage for service providers
- Support for both distribution and access network environments with the outward facing MEPs enhancement.

Note The outward facing MEPs are not supported on the ML-MR-10 card.

- Support for interoperability with CPP. Ethernet CFM will work on CPP active ports.
- Support for QoS on CFM packets.
    - 802.1p bits can be configured for the locally generated CFM packets

Note The 802.1p bit support for the CFM packets is not supported on the ML-MR-10 card.

- Locally generated CFM packets with other control packets can be queued appropriately
- Multicast packets that are forwarded by the CPU can be queued appropriately

- Support for interoperability with other Cisco routeres, such as Catalyst 3750 Metro router and Catalyst 6K.

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 34-1 on page 34-3, 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 34-2 on page 34-4, 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 34-1 CFM Maintenance Domains

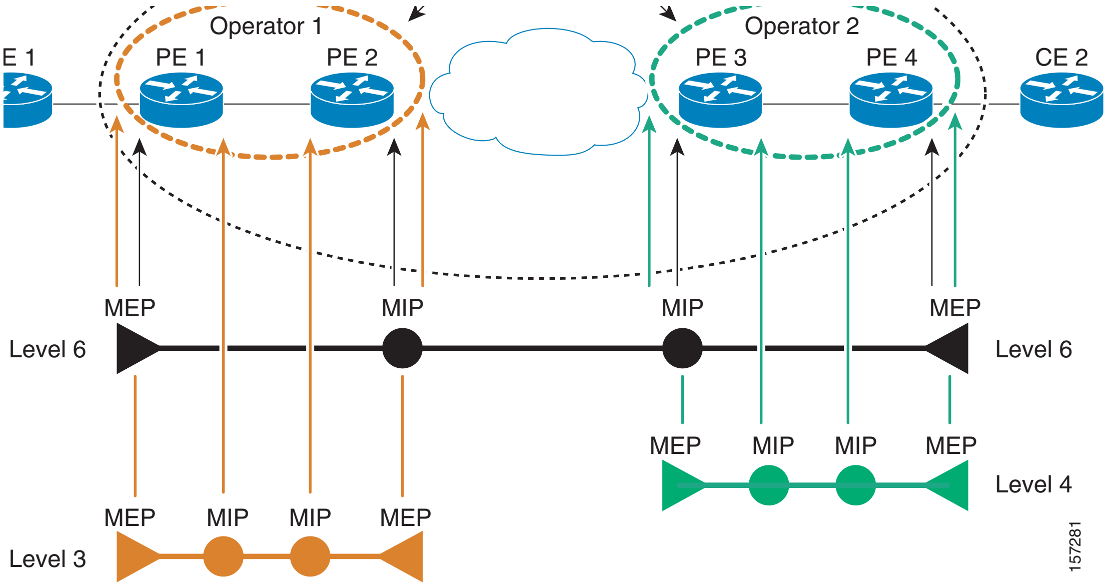
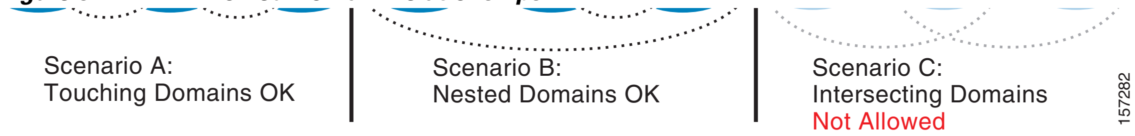


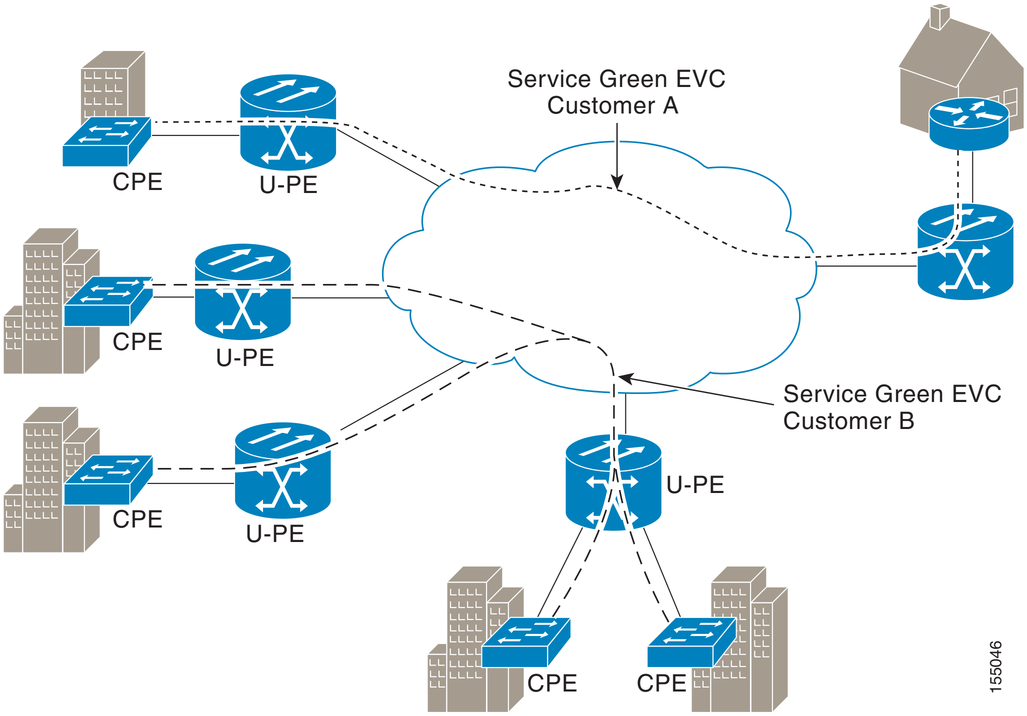
Figure 34-2 Allowed Domain Relationships



Customer Service Instance

A customer service instance is an Ethernet virtual connection (EVC), which is identified by an S-VLAN within an Ethernet island, and is identified by a globally unique service ID. A customer service instance can be point-to-point or multipoint-to-multipoint. Figure 34-3 on page 34-4 shows two customer service instances. Service Instance Green is point-to-point; Service Instance Blue is multipoint-to- multipoint.

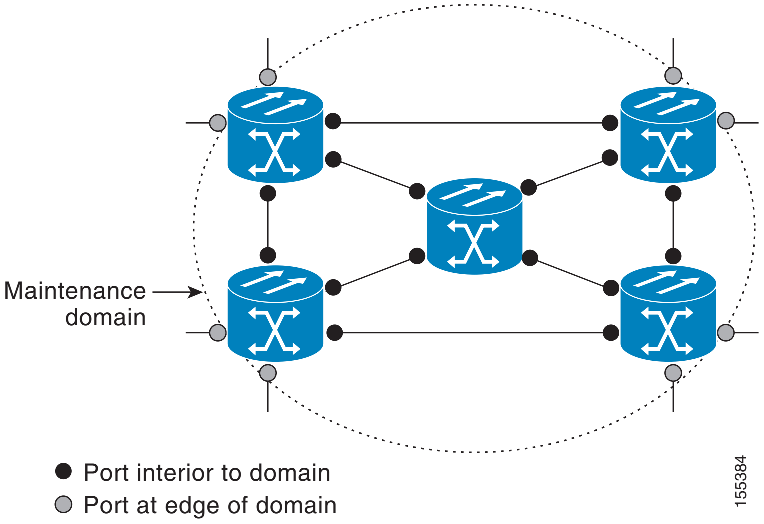
Figure 34-3 Customer Service Instances



Maintenance Domain

A maintenance domain is a management space for the purpose of managing and administering a network. A domain is owned and operated by a single entity and defined by the set of ports internal to it and at its boundary. Figure 34-4 on page 34-5 illustrates a typical maintenance domain.

Figure 34-4 Ethernet CFM Maintenance Domain



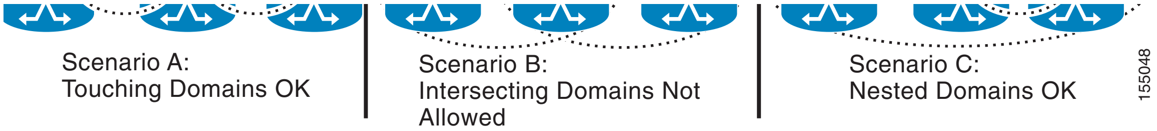
A unique maintenance level in the range of 0 to 7 is assigned to each domain by a network administrator. Levels and domain names are useful for defining the hierarchical relationship that exists among domains. The hierarchical relationship of domains parallels the structure of customer, service provider, and operator. The larger the domain, the higher the level value. For example, a customer domain would be larger than an operator domain. The customer domain may have a maintenance level of 7 and the operator domain may have a maintenance level of 0. Typically, operators would have the smallest domains and customers the largest domains, with service provider domains between them in size. All levels of the hierarchy must operate together.

Domains should not intersect because intersecting would mean management by more than one entity, which is not allowed. Domains may nest or touch but when two domains nest, the outer domain must have a higher maintenance level than the domain nested within it. Nesting maintenance domains is useful in the business model where a service provider contracts with one or more operators to provide Ethernet service to a customer. Each operator would have its own maintenance domain and the service provider would define its domain—a superset of the operator domains. Furthermore, the customer has its own end-to-end domain which is in turn a superset of the service provider domain. Maintenance levels of various nesting domains should be communicated among the administering organizations. For example, one approach would be to have the service provider assign maintenance levels to operators.

CFM exchanges messages and performs operations on a per-domain basis. For example, running CFM at the operator level does not allow discovery of the network by the higher provider and customer levels.

Network designers decide on domains and configurations. Figure 34-5 on page 34-6 illustrates a hierarchy of operator, service provider, and customer domains and also illustrates touching, intersecting, and nested domains.

Figure 34-5 Ethernet CFM Maintenance Domain Hierarchy



Maintenance Point

A maintenance point is a demarcation point on an interface that participates in CFM within a maintenance domain. Maintenance points on device ports act as filters that confine CFM frames within the bounds of a domain by dropping frames that do not belong to the correct level. Maintenance points must be explicitly configured on Cisco devices. Maintenance points drop all lower-level frames and forward all higher-level frames. There are two types of maintenance points:

A maintenance point is a demarcation point on an interface that participates in CFM within a maintenance domain. Maintenance points on device ports act as filters that confine CFM frames within the bounds of a domain by dropping frames that do not belong to the correct level. Maintenance points must be explicitly configured on Cisco devices. 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.

  On the ML-MR-10 card MIP is supported on the GigabitEthernet, POS, Port Channels, and 802.17 RPR interfaces.

Note For the current Cisco IOS implementation, a MEP of level L (where L is less than 7) requires a MIP of level M > L on the same port; hence, CFM frames at levels M to L+1 will be catalogued by this MIP.

Maintenance Intermediate Points

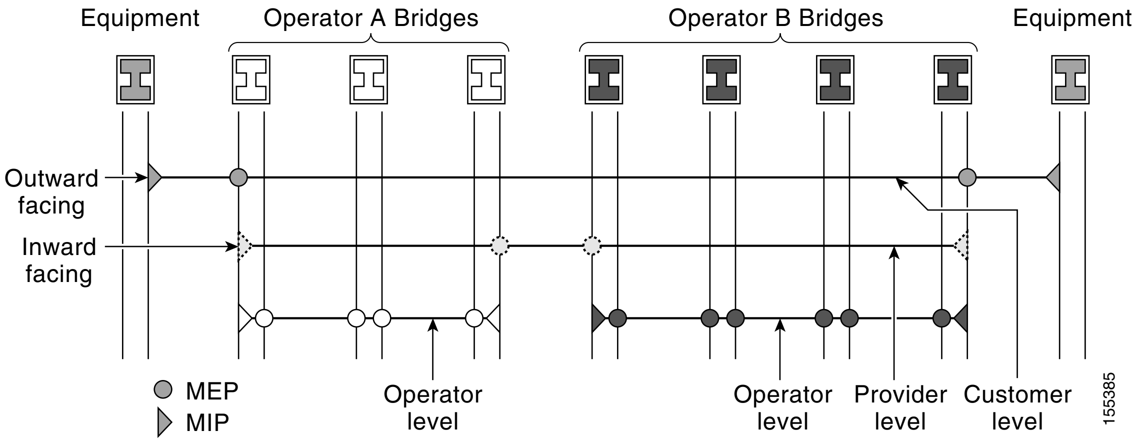
MIPs have the following characteristics:

- Per maintenance domain (level) and for all S-VLANs enabled or allowed on a port.
- Internal to a domain, not at the boundary.
- CFM frames received from MEPs and other MIPs are cataloged and forwarded, using both the wire and the relay function.
- All CFM frames at a lower level are stopped and dropped, independent of whether they originate from the wire or relay function.
- All CFM frames at a higher level are forwarded, independent of whether they arrive from the wire or relay function.
- Passive points, respond only when triggered by CFM traceroute and loopback messages.
- Bridge-Brain MAC addresses are used.

A MIP has only one level associated with it and the command-line interface (CLI) does not allow you to configure a MIP for a domain that does not exist.

Figure 34-6 illustrates MEPs and MIPs at the operator, service provider, and customer levels.

Figure 34-6 CFM MEPs and MIPs on Customer and Service Provider Equipment, Operator Devices



CFM Messages

CFM uses standard Ethernet frames. CFM frames are distinguishable by SNAP type and reserved multicast MAC address. CFM frames are sourced, terminated, processed, and relayed by bridges. Routers can support only limited CFM functions.

Bridges that cannot interpret CFM messages forward them as normal data frames. All CFM messages (except loopback) are confined to a maintenance domain and to an EVC. Three types of messages are supported:

- Continuity Check
- Loopback
- Traceroute

Continuity Check Messages

CFM continuity check messages (CCMs) are multicast heartbeat messages exchanged periodically among MEPs. They allow MEPs to discover other MEPs within a domain and allow MIPs to discover MEPs. CCMs are confined to a domain and EVC.CFM CCMs have the following characteristics:

- Transmitted at a configurable periodic interval by MEPs. The interval can be from 10 seconds to 65535 seconds, the default is 30.
- Contain a configurable hold-time value to indicate to the receiver the validity of the message. The default is 2.5 times the transmit interval.
- Catalogued by MIPs at the same or higher maintenance level.
- Terminated by remote MEPs at the same maintenance level.
- Unidirectional and do not solicit a response.
- Carry the status of the port on which the MEP is configured.

Loopback Messages

CFM loopback messages are unicast frames that a MEP transmits, at the request of an administrator, to verify connectivity to a particular maintenance point. A reply to a loopback message indicates whether a destination is reachable but does not allow hop-by-hop discovery of the path. A loopback message is similar in concept to an Internet Control Message Protocol (ICMP) Echo (ping) message.

A CFM loopback message can be generated on demand using the CLI. The source of a loopback message must be a MEP; the destination may be a MEP or a MIP. CFM loopback messages are unicast; replies to loopback messages also are unicast. CFM loopback messages specify the destination MAC address, VLAN, and maintenance domain.

Traceroute Messages

CFM traceroute messages are multicast frames that a MEP transmits, at the request of an administrator, to track the path (hop-by-hop) to a destination MEP. They allow the transmitting node to discover vital connectivity data about the path, and allow the discovery of all MIPs along the path that belong to the same maintenance domain. For each visible MIP, traceroute messages indicate ingress action, relay action, and egress action. Traceroute messages are similar in concept to User Datagram Protocol (UDP) traceroute messages.

Traceroute messages include the destination MAC address, EVC, and maintenance domain and they have Time To Live (TTL) to limit propagation within the network. They can be generated on demand using the CLI. Traceroute messages are multicast; reply messages are unicast.

Cross-Check Function

The cross-check function is a timer-driven post-provisioning service verification between dynamically discovered MEPs (via CCMs) and expected MEPs (via configuration) for a service. The cross-check function verifies that all endpoints of a multipoint or point-to-point service are operational. The function supports notifications when the service is operational; otherwise it provides alarms and notifications for unexpected endpoints or missing endpoints.

The cross-check function is performed one time. You must initiate the cross-check function from the CLI every time you want a service verification.

IOS Error Messages

The following IOS Error Messages are supported on the ML-MR-10 card:

Continuity Check Error Messages

- MEP up—Receives CCM but logged only for a state transition.
- MEP down—The entry in CCDB corresponding to this entry has timed out.
- Cross-connect—Receives CCM with unmatched CSI ID.
- Configuration Error—Receives CCM with own MPID but different Source MAC.
- Forwarding Loop—Receives CCM with own MPID and Source MAC.

Crosscheck Error Messages

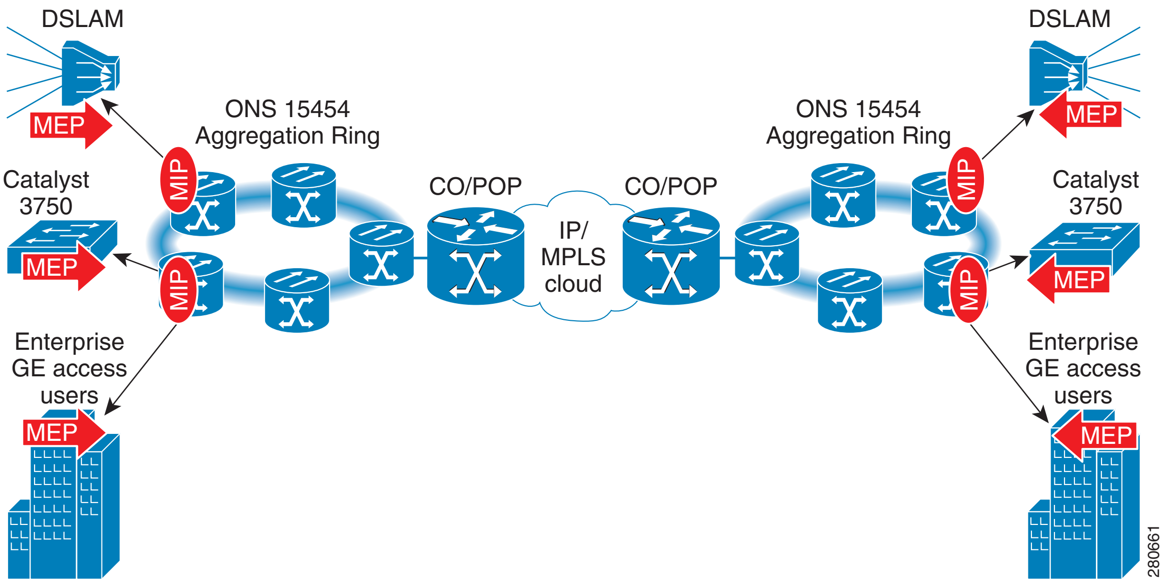
- MEP missing—The configured remote MEP does not come up during the cross-check start timeout interval.
- Unknown MEP—A CCM is received from an unexpected MEP.
- Service UP—All expected remote MEPs are up in time.

View of CFM Interaction on different Networks with ML-MR-10 Card

Customer view of CFM Network

Figure 34-7 displays the customer view of the CFM network.

Figure 34-7 Customer View of the Network

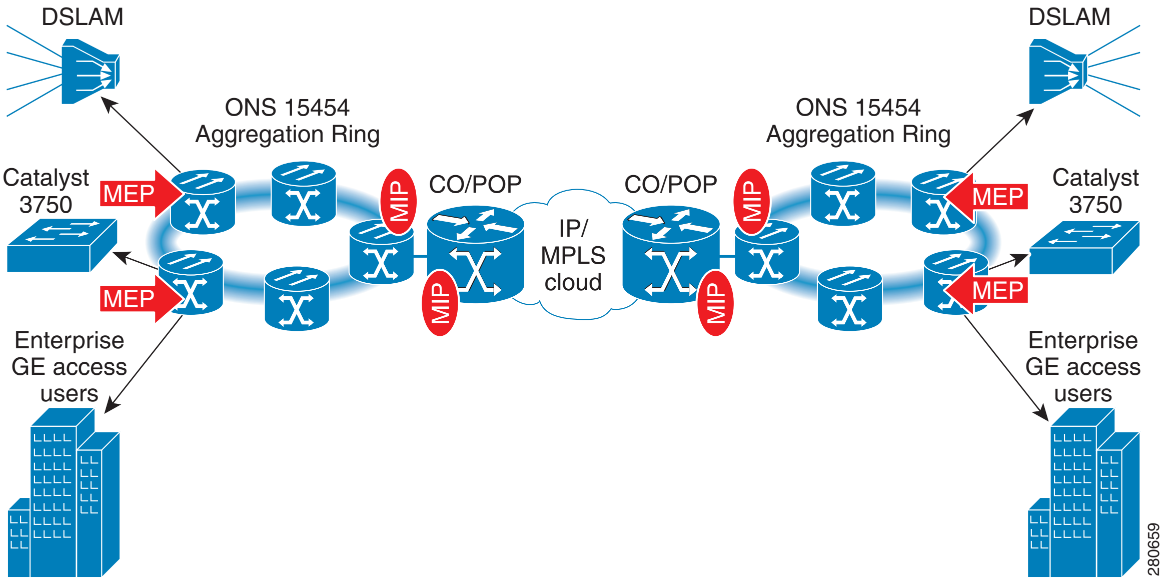


MIPs are configured on the ML-MR-10 card customer facing Gigabit Ethernet ports, Fast Ethernet ports (or) port channels.

Provider View of the Network with IP/MPLS Core

Figure 34-8 displays the provider view of the network with an IP/MPLS core.

Figure 34-8 Provider View of the Network



MEPs are configured on the ML-MR-10 card customer facing Gigabit Ethernet, Fast Ethernet ports (or) port channels.

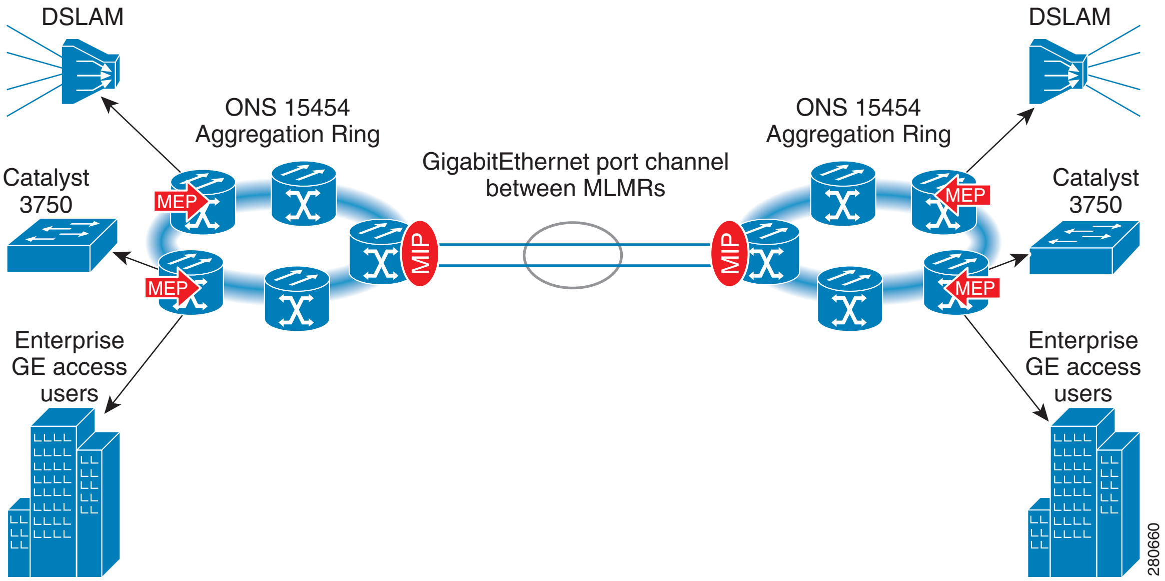
MIPs are configured on the "boundary ports" of two different operators. that is, MIPs are configuredon the ML-MR-10 card Gigabit port/Gigabit port channel, connected to a Edge router such as the Cisco 7600.

Assumption: Ring network and core IP/MPLS networks are operated by two different operators, or these networks need to be administered at a different Management Domain.

Provider View of the Network With Interconnected Rings

Figure 34-9 displays the provider view of the network with interconnected rings.

Figure 34-9 Provider View of the Network with Interconnected Rings



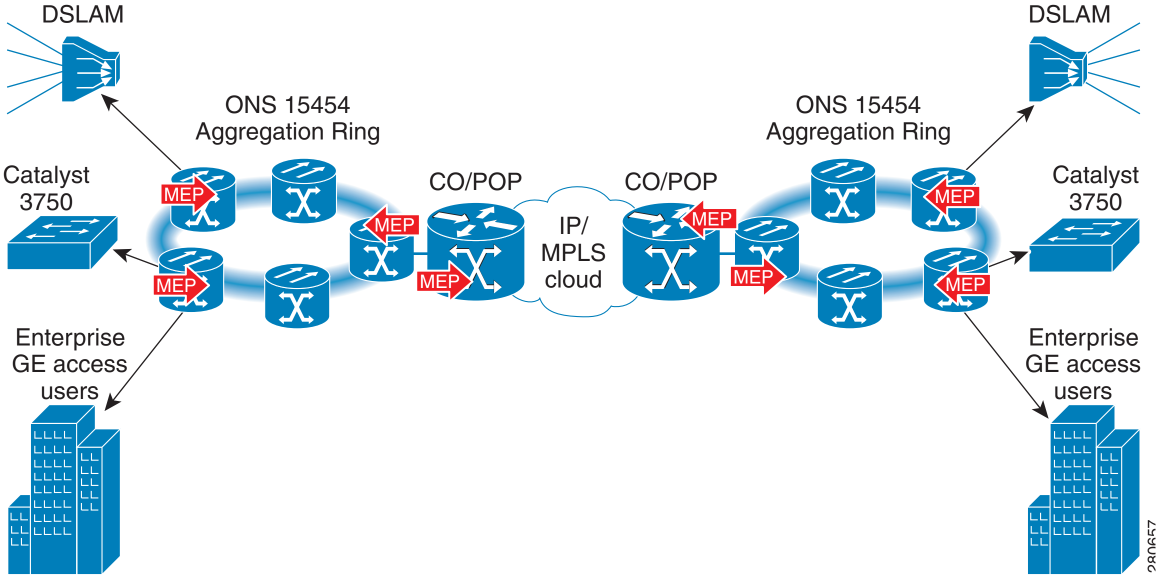
MEPs are configured on the ML-MR-10 card customer facing Gigabit Ethernet, Fast Ethernet ports (or) port channels.

MIPs are configured on the “boundary ports” of two different operators. that is., MIPs are configured on the ML-MR-10 Gigabit Ethernet Port channel, used to interconnect two rings. Assume that each ring is operated by a different operator.

34.0.0.1 Operator View of the Network with IP/MPLS Core

Figure 34-10 displays the operator view of the network with an IP/MPLS core.

Figure 34-10 Operator view of the Network with IP/MPLS Core

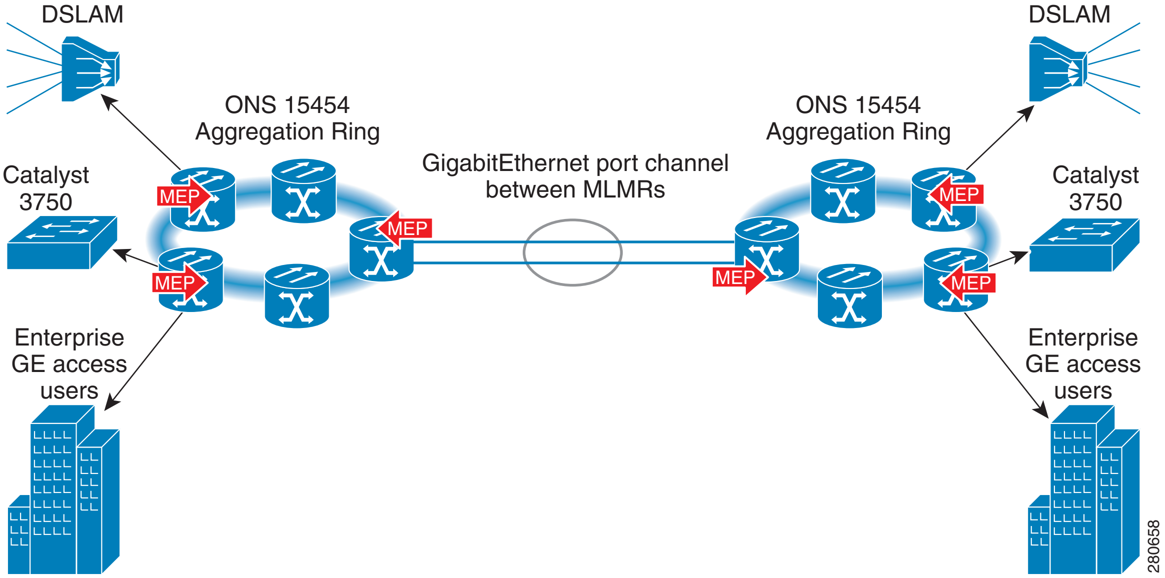


MEPs are configured on the operator's "boundary ports". that is., MEPs are configured on the ML-MR-10 card Gigabit Ethernet ports or port channels.

34.0.0.2 Operator View of the Network with Interconnected rings

Figure 34-11 displays the operator view of the network with interconnected rings.

Figure 34-11 Operator View of the Network with Interconnected Rings



MEPs are configured on the operator's "boundary ports". that is., MEPs are configured on the ML-MR-10 card Gigabit Ethernet ports or port channels.

Configuring Ethernet CFM

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

- Default Ethernet CFM Configuration, page 34-13
- Ethernet CFM Configuration Guidelines, page 34-14
- Configuring the Ethernet CFM Service, page 34-14
- Configuring Ethernet CFM Crosscheck, page 34-15

Default Ethernet CFM Configuration

The CFM is globally disabled by default. You need to enable CFM on all interfaces. A port can be configured as a flow point (MIP/MEP), a transparent port, or disabled (CFM disabled). By default, ports remain as transparent ports until configured as MEP, MIP, or disabled.

Ethernet CFM Configuration Guidelines

The following are the configuration guidelines and restrictions for CFM:

- CFM is supported on port channels. You can configure MEP/MIP on a port channel.
- CFM is supported on untagged, single tagged, and double tagged services.

Configuring the Ethernet CFM Service

To prepare the network for Ethernet CFM, do the following:

	Command	Purpose
Step 1	Router# **configure terminal**	Enters global configuration mode.
Step 2	Router(config)# **ethernet cfm enable**	Enables CFM globally.
Step 3	Router(config)# **ethernet cfm traceroute cache** [**size** *entries* | **hold-time** *minutes*]	(Optional) Configures the CFM traceroute cache. You can set a maximum cache size or hold time. • (Optional) For **size**, enter the cache **size** in number of *entry* lines. The range is from 1 to 4095; the default is 100 lines. • (Optional) For **hold-time**, enter the maximum cache **hold time** in *minutes*. The range is from 1 to 65535; the default is 100 minutes.
Step 4	Router(config)# **ethernet cfm domain** *domain-name* **level** *level-id*	Defines a CFM domain, sets the domain level, and enters ethernet-cfm configuration mode for the domain. The maintenance level number range is 0 to 7.
Step 5	Router(config-ether-cfm)# [**no**] **service csi-id evc** *evc-name*	Sets a universally unique ID for the customer within a maintenance domain for an EVC.
Step 6	Router(config-ether-cfm)# **mep archive-hold-time** *minutes*	(Optional) Sets the number of minutes that data from a missing maintenance end point (mep) is kept before it is purged. The range is 1 to 65535; the default is 100 minutes.
Step 7	Router(config-ether-cfm)# **exit**	Returns to global configuration mode.
Step 8	Router(config)# **interface** *interface-id*	Specifies a physical interface or a port channel to configure, and enters interface configuration mode.
Step 9	Router(config-if)# **ethernet cfm mip level** *level-id*	Configures an operator-level maintenance intermediate point (MIP) for the domain level-ID defined in Step 4. **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 10	Router(config-if)# **service instance** *instance-id* **ethernet** *evc-id*	Creates service instance on an interface and sets the device into the config-if-srv submode.
Step 11	Router(config-if-srv)# **encapsulation dot1q** *value*	Defines the matching criteria to be used to map ingress frames on an interface to the appropriate service instance.
Step 12	Router(config-if-srv)# **bridge-domain number**	Binds the service instance to a bridge domain instance where bridge-id is the identifier for the bridge domain instance.

	Command	Purpose
Step 13	Router(config-if-srv)# [**no**] **ethernet cfm mep domain** *domain-name* {[**inward** | **outward**]} **mpid** *id* [**cos** *cos_value*]	(Optional) Defines a maintenance port with the desired direction on a port in the maintenance domain.
Step 14	**exit**	Returns to global configuration mode.
Step 15	Router(config)# **[no] ethernet cfm cc enable level** {**any** | *level-id* | *level-id-level-id*} **evc** *evc-name*	Configures per domain continuity check (cc) parameters. The level ID identifies the domain to which configuration applies. • Enter **enable** to enable CFM cc for the domain level. • Enter a maintenance **level** as a level number (0 to 7) or as **any** for all maintenance levels. • Enter the VLANs to apply the check to, as a VLAN-ID (1 to 4095), a range of VLAN-IDs separated by a hyphen, a series of VLAN IDs separated by commas, or **any** for any VLANs.
Step 16	Router(config)# **end**	Returns to privileged EXEC mode.
Step 17	Router# **show ethernet cfm domain brief** Router# **show ethernet cfm maintenance-points local** Router# **show ethernet cfm traceroute-cache**	Verifies the configuration.
Step 18	Router# **show running-config**	Verifies your entries.
Step 19	Router# **copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

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

Configuring Ethernet CFM Crosscheck

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

	Command	Purpose
Step 1	Router# **configure terminal**	Enters global configuration mode.
Step 2	Router(config)# **ethernet cfm mep crosscheck start-delay** *delay*	Configures the number of seconds that the device waits for remote MEPs to come up before the crosscheck is started. The range is 1 to 65535; the default is 30 seconds.
Step 3	Router(config)# **ethernet cfm domain** *domain-name* **level** *level-id*	Defines a CFM domain, set the domain level, and enter ethernet-cfm configuration mode for the domain. The maintenance level number range is 0 to 7.
Step 4	Router(config)# **[no] mep crosscheck mpid** *id* **evc** *evc-name* [**mac** *mac-address*]	Defines a remote MEP within a maintenance domain. • For **mpid** *id*, enter the remote MEP's maintenance end point identifier. The range is 1 to 8191. • For EVC ***evc-name***, specify the name you want to crosscheck. • (Optional) Specify the MAC address of the remote MEP.

	Command	Purpose
Step 5	`Router(config)# end`	Returns to privileged EXEC mode.
Step 6	`Router# ethernet cfm mep crosscheck {enable	disable} level {level-id	level-id-level-id } evc evc-name`	Enable or disable CFM crosscheck for one or more maintenance levels and EVCs. • 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 EVC ***evc-name***, specify the name you want to crosscheck.
Step 7	`Router# show ethernet cfm maintenance-points remote crosscheck`	Verifies the configuration.
Step 8	`Router# show ethernet cfm errors`	Enters this command after you enable CFM crosscheck to display the results of the crosscheck operation.
Step 9	`Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring Examples for CFM

The following sections provide examples for configuring CFM:

- CFM with Inward Facing MEPs, page 34-16
- Configuring and Enabling Cross-Checking on Inward Facing MEP, page 34-17
- Ping Utility in the Ethernet Network, page 34-18
- Traceroute Utility in the Ethernet Network, page 34-18

CFM with Inward Facing MEPs

This example illustrates how to configure CFM with an inward facing MEP:

On Router 1

```
configure terminal
ethernet cfm enable
ethernet cfm domain customer_domain level 7
ethernet cfm domain PROVIDER_DOMAIN level 4
service customerX evc evc_1

interface GigabitEthernet0
ethernet cfm mip level 7
service instance 10 ethernet evc_1
encapsulation dot1q 102
bridge-domain 100
cfm mep domain PROVIDER_DOMAIN inward mpid 1101
exit


interface rpr 0
service instance 12 ethernet evc_1
encapsulation dot1q 102
bridge-domain 100
exit

ethernet cfm cc enable level 4 evc evc_1
```

On Router 2

```
configure terminal
ethernet cfm enable
ethernet cfm domain customer_domain level 7
ethernet cfm domain PROVIDER_DOMAIN level 4
service customerX evc evc_1

interface GigabitEthernet0
ethernet cfm mip level 7
service instance 10 ethernet evc_1
encapsulation dot1q 102
bridge-domain 100
cfm mep domain PROVIDER_DOMAIN inward mpid 1102
exit

interface rpr 0
service instance 12 ethernet evc_1
encapsulation dot1q 102
bridge-domain 100
exit

ethernet cfm cc enable level 4 evc evc_1
```

Configuring MEP on the Transit Router

```
======================================
configure terminal
ethernet cfm enable
ethernet cfm domain PROVIDER_DOMAIN level 4
service customerX evc evc_1

interface GigabitEthernet0
ethernet cfm mip level 4
service instance 12 ethernet evc_1
encapsulation dot1q 102
bridge-domain 100
exit
```

Configuring and Enabling Cross-Checking on Inward Facing MEP

Configuring Cross-Checking on an Inward Facing MEP

```
U-PE A
```

```
ethernet cfm domain ServiceProvider level 4
mep crosscheck mpid 402 evc_1
!
ethernet cfm mep crosscheck start-delay 60
```

```
U-PE B
```

```
ethernet cfm domain ServiceProvider level 4
mep crosscheck mpid 401 evc_1
!
ethernet cfm mep crosscheck start-delay 60
```

Enabling Cross-Checking on an Inward Facing MEP

```
U-PE A
```

U-PEA# **ethernet cfm mep crosscheck enable level 4 evc_1**

```
U-PE B
```

```
U-PEB# ethernet cfm mep crosscheck enable level 4 evc_1
```

Ping Utility in the Ethernet Network

The Ping utility is used to troubleshoot the accessibility of the network elements.The CFM extends the Ping utility to Ethernet networks also.

Ping the MEPs:

```
Router# ping ethernet mpid 10 level 2 evc evc_6
    Type escape sequence to abort.
Sending 5 Ethernet CFM loopback messages, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

Ping the MIPs:

Use a bridge-brain MAC address to ping an MIP in an Ethernet network, because they do not have a configured MPID."

```
Router# ping ethernet 0019.076c.838f level 2 evc evc_6
    Type escape sequence to abort.
Sending 5 Ethernet CFM loopback messages, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Traceroute Utility in the Ethernet Network

The t**raceroute** command is used to find out the actual routes taken by the packets to reach the destination. The **traceroute** command is also used to isolate a problem in the Ethernet networks related to packets failing to reach the destination. The CFM extends the traceroute utility to the Ethernet networks also.

```
MLMR-5# traceroute ethernet  0019.076c.838f level 2 evc evc_6

Type escape sequence to abort. TTL 255. Per-Hop Timeout is 10 seconds
Tracing the route to 0019.076c.838f on Domain OperatorC, Level 2, evc evc_6
Traceroute sent via RPR-IEEE0


B = Intermediary Bridge
! = Target Destination
* = Per Hop Timeout
------------------------------------------------------------------------------

                      MACMAC      Ingress     Ingr Action  Relay Action

Hops   Host            Forwarded   Egress      Egr Action   Next Hop

------------------------------------------------------------------------------

! 1  MLMR-15         0019.076c.838f                      RlyNone

                 Not Forwarded
```

Troubleshooting Tips

To verify and isolate a fault on the maintenance domain, start at the highest level maintenance domain and perform the following steps:

Step 1 Check the device error status.

Step 2 When a error exists, perform a loopback test to confirm the error.

Step 3 Run a traceroute to the destination to isolate the fault.

Step 4 Correct the fault when it is identified.

Step 5 If the fault is not identified, go to the next lower maintenance domain and repeat Step 1 to Step 4 at that maintenance domain level.

Repeat Step 1 to Step 4, as needed, to identify and correct the fault.

Displaying Ethernet CFM Information

You can use the privileged EXEC commands in Table 34-1 to display Ethernet CFM information.

Table 34-1 Displaying CFM Information

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

Understanding the Ethernet OAM (IEEE 802.3ah) Protocol

The Ethernet OAM (IEEE 802.3ah) 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 (IEEE 802.3ah). You can implement Ethernet OAM(IEEE 802.3ah) 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 (IEEE 802.3ah) 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(IEEE 802.3ah) 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 ML-MR-10 card supports Ethernet OAM discovery as per the IEEE 802.3ah standards.
- 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

The following 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.
- The ML-MR-10 card supports receiving and processing the RFI as per IEEE 802.3ah standard and the following failure conditions are supported:
  - Link Fault
  - Dying Gasp
  - Critical Event
- The ML-MR-10 card detects and sends the Dying Gasp Remote Failure Indication (RFI) upon detecting conditions consistent across the Cisco platforms. The following conditions trigger the Dying Gasp RFI:
  - Administrative shutdown of the interface
  - Reload of the card
  - Deconfiguration of IEEE 802.3ah on the interface
- Error-blocking state indicates that the interface will not receive or send any data traffic, though it will continue to listen to the IEEE 802.3ah packets. When the peer returns to the normal condition (from error state to normal) and resets the RFI condition, the interface comes UP and traffic passes smoothly.

- During the transition to error-blocking state, if the interface is CPP protected, the interface will be forced to operational DOWN immediately (instead of waiting for the failure, which will be reported by the driver at a later moment) thus triggering the CPP to route the traffic to a Standby port.
- The ML-MR-10 card supports enabling or disabling Link Monitoring per interface.
- The ML-MR-10 card supports error notification for the following events as per IEEE 802.3ah standard:
  - Errored Frame
  - Errored Frame Period
  - Errored Frame Seconds Summary
  - Cisco proprietary Receive CRC errors
- The management interfaces support the following 802.3ah event when an Ethernet interface is configured for 802.3ah OAM:
  - Critical events: These event cause the CTC or TL1 to report as major alarms while Cisco IOS generates SysLog messages. Link Fault, Dying Gasp and Critical Event RFIs are considered Critical events.
  - Transient Conditions: The locally detected Link Monitoring events are reported to CTC or TL1 as Transient conditions, which are: Errored Frame, Errored Frame Period, Errored Frame Seconds Summary, and Cisco proprietary Receive CRC errors.
- SNMP reports both the Critical events and Transient conditions using the cdot3OamEventLogTable of the CISCO-DOT3-OAM-MIB.
- Remote loopback mode ensures link quality with a remote peer during installation or troubleshooting. In this mode, when the ML-MR-10 card 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.
  - The ML-MR-10 card supports enabling or disabling Remote Loopback on the Front end Ethernet interface as per the IEEE 802.3ah standard.
- The ML-MR-10 card supports IEEE 802.3ah on CPP Active ports and Standby-ON ports.
- The IETF MIB (Cisco-Dot3-OAM-MIB) for IEEE 802.3ah is supported.
- The ML-MR-10 card supports interoperability with Cisco Metro routers, such as Catalyst 3750 and Catalyst 6K.
- The ML-MR-10 card allows configuring IEEE 802.3ah and work on all of its front end interfaces.
- The ML-MR-10 card allows configuring IEEE 802.3ah on the member interfaces of a port channel.

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 (IEEE 802.3ah)

This section includes the following information about Ethernet OAM (IEEE 802.3ah):

Default Ethernet OAM (IEEE 802.3ah) 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 (IEEE 802.3ah) Configuration Guidelines

Follow these guidelines when configuring Ethernet OAM:

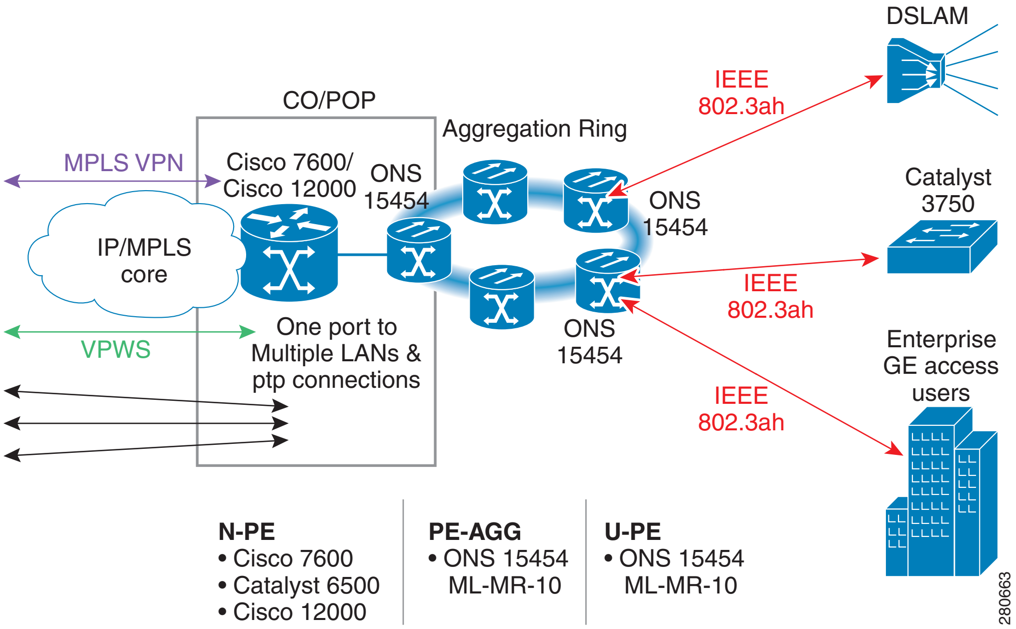
- The ML-MR-10 card does not support monitoring of egress frames sent with cyclic redundancy code (CRC) errors. The **ethernet oam link-monitor transmit crc** interface-configuration and template-configuration commands are visible but are not supported on the router. The commands are accepted, but are not applied to an interface.
- For a remote failure indication, the router does not generate Link Fault or Critical Event OAM PDUs. However, if these PDUs are received from a link partner, they are processed. The router 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 router is reloading. It can respond to, but not generate, Dying Gasp PDUs based on loss of power.
- The ML-MR-10 card does not support Ethernet OAM on ports that belong to an EtherChannel.
- The ML-MR-10 card supports the following IEEE 802.3ah requirements on the following interfaces:
  - Front end Ethernet interface
  - Front end Ether interface, which is a member of a port channel
- The ML-MR-10 card monitors the frames received with cyclic redundancy code (CRC) errors and displays the CRC error threshold crossing information in the error log files. Use Cisco IOS to view the log files.

  If you have not enabled error logging, check autonomous messages in the Cisco IOS session. For more information about autonomous messages, refer to *Cisco ONS SONET TL1 Reference Guide*.

Deployment of EOAM (IEEE 802.3ah) with an ML-MR-10 card

Figure 34-12 on page 34-23 displays the deployment of EOAM on an ML-MR-10 card.

Figure 34-12 Deployment of IEEE 802.3ah with ML-MR-10 card



Enabling Ethernet OAM (IEEE 802.3ah) on an Interface

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

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

	Command	Purpose
Step 4	`Router # ethernet oam [max-rate oampdus	min-rate seconds	mode {active	passive}	timeout seconds]`	You can configure these optional OAM parameters: • (Optional) Enter **max-rate** *oampdus* to configure the maximum number of OAM PDUs sent per second. The range is from 1 to 10. • (Optional) Enter **min-rate** *seconds* to configure the minimum transmission rate in seconds when one OAM PDU is sent per second. The range is from 1 to 10. • (Optional) Enter **mode active** to set OAM client mode to active. • (Optional) Enter **mode passive** to set OAM client mode to passive. **Note** When Ethernet OAM mode is enabled on two interfaces passing traffic, at least one must be in the active mode. • (Optional) Enter **timeout** *seconds* to set a time for OAM client timeout. The range is from 2 to 30.
Step 5	`Router # end`	Return to privileged EXEC mode.
Step 6	`Router # show ethernet oam status [interface interface-id]`	Verify the configuration.
Step 7	`Router # 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 (IEEE 802.3ah) 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 the following limitation:

- Internet Group Management Protocol (IGMP) packets are not looped back.

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

	Command	Purpose
Step 1	`Router # configure terminal`	Enter global configuration mode.
Step 2	`Router # interface interface-id`	Define an interface to configure as an EOM interface, and enter interface configuration mode.
Step 3	`Router # ethernet oam remote-loopback {supported	timeout seconds}`	Enable Ethernet remote loopback on the interface or set a loopback timeout period. • Enter **supported** to enable remote loopback. • Enter **timeout** *seconds* to set a remote loopback timeout period. The range is from 1 to 10 seconds.

	Command	Purpose
Step 4	`Router # end`	Return to privileged EXEC mode.
Step 5	`Router # ethernet oam remote-loopback {start	stop} {interface interface-id}`	Turn on or turn off Ethernet OAM remote loopback on an interface.
Step 6	`Router # show ethernet oam status [interface interface-id]`	Verify the configuration.
Step 7	`Router # 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 (IEEE 802.3ah) 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	`Router # configure terminal`	Enter global configuration mode.
Step 2	`Router # interface interface-id`	Define an interface, and enter interface configuration mode.
Step 3	`Router # 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.
Step 4	`Router # ethernet oam link-monitor symbol-period {threshold {high {high symbols	none}	low {low-symbols}}	window symbols}` `Repeat this step to configure both high and low thresholds.`	(Optional) Configure high and low thresholds for an error-symbol period that trigger an error-symbol period link event. • Enter **threshold high** *high-symbols* to set a high threshold in number of symbols. The range is 1 to 65535. The default is **none**. • Enter **threshold high none** to disable the high threshold if it was set. This is the default. • Enter **threshold low** *low-symbols* to set a low threshold in number of symbols. The range is 0 to 65535. It must be lower than the high threshold. • Enter **window** *symbols* to set the window size (in number of symbols) of the polling period. The range is 1 to 65535 symbols.

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

	Command	Purpose

Step 8	`Router #` **`ethernet oam link-monitor receive-crc`** {**`threshold`** {**`high`** {*`high-frames`* | **`none`**} | **`low`** {*`low-frames`*}} | **`window`** *`milliseconds`*}
	`Repeat this step to configure both high and low thresholds.`
		(Optional) Configure thresholds for monitoring ingress frames received with CRC errors for a period of time.
		• Enter **threshold high** *high-frames* to set a high threshold for the number of frames received with CRC errors. The range is 1 to 65535 frames.
		• Enter **threshold high none** to disable the high threshold.
		• Enter **threshold low** *low-frames* to set a low threshold in number of frames. The range is 0 to 65535. The default is 1.
		• Enter **window** *milliseconds* to set the a window and period of time during which frames with CRC errors are counted. The range is 10 to 1800 and represents the number of milliseconds in multiples of 100. The default is 100.

Step 9	`Router #` **`[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	`Router #` **`end`**	Return to privileged EXEC mode.
Step 11	`Router #` **`show ethernet oam status`** [**`interface`** *`interface-id`*]	Verify the configuration.
Step 12	`Router #` **`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 router 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 (IEEE 802.3ah) 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	`Router #` **`configure terminal`**	Enter global configuration mode.
Step 2	`Router #` **`interface`** *`interface-id`*	Define an interface, and enter interface configuration mode.

	Command	Purpose
Step 3	`Router # 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: • 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	`Router # end`	Return to privileged EXEC mode.
Step 5	`Router # show ethernet oam status [interface interface-id]`	Verify the configuration.
Step 6	`Router # copy running-config startup-config`	(Optional) Save your entries in the configuration file.

The ML-MR-10 card does not generate Link Fault or Critical Event OAM PDUs. However, if these PDUs are received from a link partner, they are processed. The router 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 router 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 (IEEE 802.3ah) 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	Router # **configure terminal**	Enter global configuration mode.
Step 2	Router # **template** *template-name*	Create a template, and enter template configuration mode.

	Command	Purpose
Step 3	`Router #` **ethernet oam link-monitor receive-crc** {**threshold** {**high** {*high-frames* | **none**} | **low** {*low-frames*}} | **window** *milliseconds*}	(Optional) Configure thresholds for monitoring ingress frames received with cyclic redundancy code (CRC) errors for a period of time. • Enter **threshold high** *high-frames* to set a high threshold for the number of frames received with CRC errors. The range is 1 to 65535 frames. • Enter **threshold high none** to disable the high threshold. • Enter **threshold low** *low-frames* to set a low threshold in number of frames. The range is 0 to 65535. The default is 1. • Enter **window** *milliseconds* to set the a window and period of time during which frames with CRC errors are counted. The range is 10 to 1800 and represents the number of milliseconds in multiples of 100. The default is 100.
Step 4	`Router #` **ethernet oam link-monitor symbol-period** {**threshold** {**high** {*high symbols* | **none**} | **low** {*low-symbols*}} | **window** *symbols*}	(Optional) Configure high and low thresholds for an error-symbol period that triggers an error-symbol period link event. • Enter **threshold high** *high-symbols* to set a high threshold in number of symbols. The range is 1 to 65535. • Enter **threshold high none** to disable the high threshold. • Enter **threshold low** *low-symbols* to set a low threshold in number of symbols. The range is 0 to 65535. It must be lower than the high threshold. • Enter **window** *symbols* to set the window size (in number of symbols) of the polling period. The range is 1 to 65535 symbols.
Step 5	`Router #` **ethernet oam link-monitor frame** {**threshold** {**high** {*high-frames* | **none**} | **low** {*low-frames*}} | **window** *milliseconds*}	(Optional) Configure high and low thresholds for error frames that trigger an error-frame link event. • Enter **threshold high** *high-frames* to set a high threshold in number of frames. The range is 1 to 65535. You must enter a high threshold. • Enter **threshold high none** to disable the high threshold. • Enter **threshold low** *low-frames* to set a low threshold in number of frames. The range is 0 to 65535. The default is 1. • Enter **window** *milliseconds* to set the a window and period of time during which error frames are counted. The range is 10 to 600 and represents the number of milliseconds in a multiple of 100. The default is 100.

	Command	Purpose
Step 6	`Router #` **ethernet oam link-monitor frame-period** {**threshold** {**high** {*high-frames* | **none**} | **low** {*low-frames*}} | **window** *frames*}	(Optional) Configure high and low thresholds for the error-frame period that triggers an error-frame-period link event. • Enter **threshold high** *high-frames* to set a high threshold in number of frames. The range is 1 to 65535. You must enter a high threshold. • Enter **threshold high none** to disable the high threshold. • Enter **threshold low** *low-frames* to set a low threshold in number of frames. The range is 0 to 65535. The default is 1. • Enter **window** *frames* to set the a polling window size in number of frames. The range is 1 to 65535; each value is a multiple of 10000 frames. The default is 1000.
Step 7	`Router #` **ethernet oam link-monitor frame-seconds** {**threshold** {**high** {*high-seconds* | **none**} | **low** {*low-seconds*}} | **window** *milliseconds*}	(Optional) Configure frame-seconds high and low thresholds for triggering an error-frame-seconds link event. • Enter **threshold high** *high-seconds* to set a high threshold in number of seconds. The range is 1 to 900. You must enter a high threshold. • Enter **threshold high none** to disable the high threshold. • Enter **threshold low** *low-frames* to set a low threshold in number of frames. The range is 1 to 900. The default is 1. • Enter **window** *frames* to set the a polling window size in number of frames. The range is 100 to 9000; each value is a multiple of 100 milliseconds. The default is 1000.
Step 8	`Router #` **ethernet oam link-monitor high threshold action error-disable-interface**	(Optional) Configure the router to put an interface in an error disabled state when a high threshold for an error is exceeded.
Step 9	`Router #` **exit**	Return to global configuration mode.
Step 10	`Router #` **interface** *interface-id*	Define an Ethernet OAM interface, and enter interface configuration mode.
Step 11	`Router #` **source-templat**e *template-name*	Associate the template to apply the configured options to the interface.
Step 12	`Router #` **end**	Return to privileged EXEC mode.
Step 13	`Router #` **show ethernet oam status** [**interface** *interface-id*]	Verify the configuration.
Step 14	`Router #` **copy running-config startup-config**	(Optional) Save your entries in the configuration file.

The router 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 router and you can enter it, but it is not supported. Use the **no** form of each command to remove the option from the template. Use the **no source-template** *template-name* command to remove the source template association.

Displaying Ethernet OAM (IEEE 802.3ah) Protocol Information

You can use the privileged EXEC commands in Table 34-2 to display Ethernet OAM protocol information.

Table 34-2 Displaying Ethernet OAM Protocol Information

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

Ethernet Local Management Interface (E-LMI)

Ethernet Local Management Interface (LMI) is an Ethernet layer operation, administration, and management (OAM) protocol. It provides information that enables autoconfiguration of customer edge (CE) devices and provides the status of Ethernet virtual connections (EVCs) for large Ethernet metropolitan-area networks (MANs) and WANs. Specifically, Ethernet LMI notifies a CE device of the operating state of an EVC and the time when an EVC is added or deleted. Ethernet LMI also communicates the attributes of an EVC and a user-network interface (UNI) to a CE device.

Prerequisites for E-LMI

The following are the prerequisites for working on the E-LMI interface:

- Ethernet OAM such as connectivity fault management (CFM) must be implemented and operational on the service provider's network.
- Ethernet LMI relies on Ethernet CFM for the status of an EVC, the remote UNI identifier associated with an EVC, and remote UNI status.

Before you set up Ethernet LMI, you should understand the following concepts:

- EVC
- Ethernet LMI

EVC

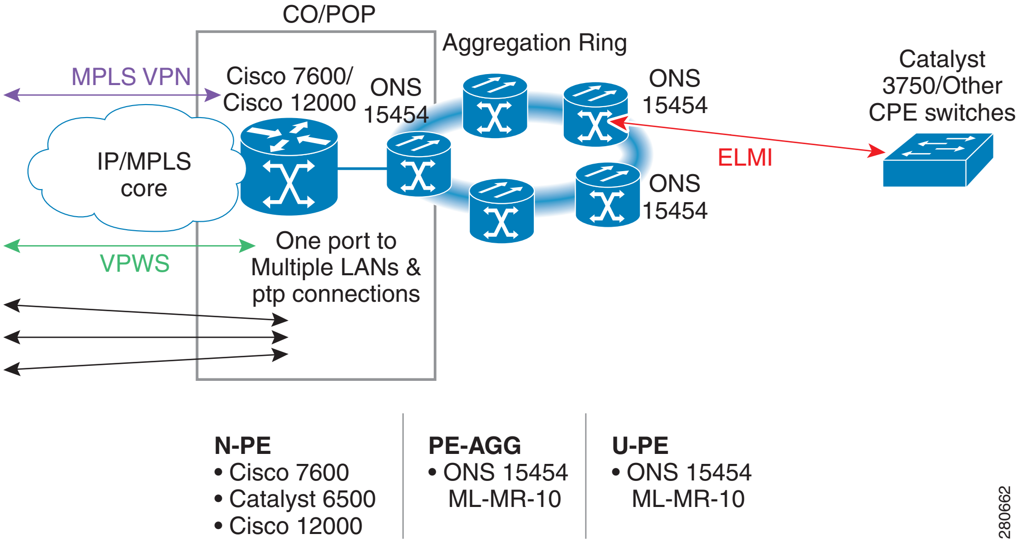
An EVC as defined by the Metro Ethernet Forum could be a port level point-to-point or multipoint-to-multipoint Layer 2 circuit. EVC status can be used by the CE device to find an alternative path in to the service provider network or in some cases, fall back to a backup path over Ethernet or another alternative service such as Frame Relay or ATM.

Ethernet LMI

Ethernet LMI is an Ethernet layer OAM protocol between a CE device and the PE in large Ethernet MANs and WANs. E-LMI provides information that enables service providers to auto configure CE devices with service parameters and parameter changes from a user provider edge (UPE) device.

Figure 34-13 shows where in a network Ethernet LMI functions.

Figure 34-13 E-LMI Functionality with Various Networks



E-LMI also provides the status of Ethernet EVCs in large Ethernet MANs and WANs to the CE. Specifically, Ethernet LMI notifies a CE device of the operating state of an EVC and the time when an EVC is added or deleted. Ethernet LMI also communicates EVC and UNI attributes to a CE device.

The Ethernet LMI protocol includes the following procedures, as defined by the MEF 16 Technical Specification:

- Notifying the CE when an EVC is added
- Notifying the CE when an EVC is deleted
- Notifying the CE of the availability state of a configured EVC (Active, Not Active, or Partially Active)
- Communicating UNI and EVC attributes to the CE

Benefits of Ethernet LMI

Ethernet LMI provides the following benefits:

- Communication of end-to-end status of the EVC to the CE device. The following EVC status can be notified to the CE device.
  - Active
  - Not Active
  - Partially Active for MP2MP services
- Communication of EVC and UNI attributes to a CE device
- Competitive advantage for service providers

Understanding E-LMI

Ethernet Local Management Interface (E-LMI) is a protocol between the CE device and the 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 router. 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. The type of information relayed is:

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

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

The following sections provide information about OAM Manager interaction with E-LMI and CFM:

- "E-LMI Interaction with the OAM Manager" section on page 34-36
- "CFM Interaction with the OAM Manager" section on page 34-36

E-LMI Features

The following are the ELMI features supported by the ML-MR-10 card:

- Support for E-LMI PE functionality. However, CE functionality is not supported.
- Support for E-LMI on CPP active ports.
- Support for E-LMI on the front end Ethernet interfaces and front end Ethernet port Channels.
- Support for interoperability with Cisco routers.

- Enable and disable capability of E-LMI functionality is supported globally.
- Support for CFM Interworking with E-LMI. The following parameters are supported with the synchronous and asynchronous E-LMI updates:
  - EVC status for both point-to-point and multi-point EVCs
  - Remote UNI name and its status
  - The number of UNIs expected in the EVC
  - Actual number of UNIs that are active

E-LMI Interaction with the OAM Manager

On the CE side, no interactions are required between the E-LMI and the OAM manager. 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 router. 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 the 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 the 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. The 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 EVCs, Ethernet Flow Point (EFPs), and E-LMI customer VLAN mapping. Most of the configuration occurs on the PE router on the interfaces connected to the CE device. On the CE router, 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 the following information about configuring E-LMI:

- Default E-LMI Configuration, page 34-37
- E-LMI and the OAM Manager Configuration Guidelines, page 34-37

- Configuring the OAM Manager, page 34-37
- Enabling E-LMI, page 34-40
- Ethernet OAM Manager Configuration Example, page 34-41
- Displaying E-LMI and OAM Manager Information, page 34-42
- Ethernet CFM and Ethernet OAM Interaction, page 34-42

Default E-LMI Configuration

The Ethernet LMI is disabled by default globally. When you enable E-LMI, the router is in PE mode by default.

- When you enable E-LMI globally by entering the E-LMI 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 the 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.

Configuring the OAM Manager

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

	Command	Purpose
Step 1	`Router #` **`configure terminal`**	Enter global configuration mode.
Step 2	`Router #` **`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	`Router #` **`service`** *`csi-id`* **`evc`** *evc-id*	Define a universally unique customer service instance (CSI) and EVC ID within the maintenance domain. • *csi-id*—A string of no more than 100 characters that identifies the CSI. • *evc-id*—A string of no more than 100 characters that identify a service. You cannot use the same evc_id for more than one domain at the same level.
Step 4	`Router #` **`exit`**	Return to global configuration mode.
Step 5	`Router #` **`ethernet evc`** *`evc-id`*	Define an EVC and enter evc configuration mode. The identifier can be up to 100 characters in length.

	Command	Purpose
Step 6	Router **# oam protocol cfm domain** *domain-name*	Configure the EVC OAM protocol as CFM, and identify the CFM domain maintenance level as configured in Step 2 and Step 3. **Note** If the CFM domain does not exist, the command is rejected, and an error message appears.
Step 7	Router **# 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 might show as active, even if all end points are not up.
Step 8	Router **# exit**	Return to global configuration mode.
Step 9	Repeat Steps 2 to 5 for other CFM domains that you want the OAM manager to monitor.	
Step 10	Router **# interface** *interface-id*	Specify a physical interface connected to the CE device, and enter interface configuration mode.
Step 11	Router **# service instance** *efp-identifier* **ethernet** [*evc-id*]	Configure an 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	Router **# 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-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	Router **# exit**	Return to interface configuration mode.

	Command	Purpose
Step 14	`Router # 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	`Router # ethernet uni {bundle [all-to-one] | multiplex}`	(Optional) Set UNI bundling attributes: • If you enter **bundle** with the text, the UNI supports bundling without multiplexing (only one EVC with one or multiple VLANs 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	`Router # end`	Return to privileged EXEC mode.
Step 17	`Router # show ethernet service evc {detail | id evc-id | interface interface-id}`	Verify the configuration.
Step 18	`Router # 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

You can enable E-LMI globally or on an interface and you can configure the router as a PE or a CE device. Beginning in privileged EXEC mode, follow these steps to enable for E-LMI on the router 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	`Router` **# configure terminal**	Enter global configuration mode.
Step 2	`Router` **# ethernet lmi global**	Globally enable E-LMI on all interfaces. By default, the router is a PE device.
Step 3	`Router` **# ethernet lmi ce**	(Optional) Configure the router as an E-LMI CE device.
Step 4	`Router` **# interface** *interface-id*	Define an interface to configure as an E-LMI interface, and enter interface configuration mode.
Step 5	`Router` **# 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 6	`Router` **# ethernet lmi** {**n391** *value* | **n393** *value* | **t391** *value*| **t392** *value*}	Configure E-LMI parameters for the UNI. The keywords have these meanings: • **n391** *value*—Set the event counter on the customer equipment. The counter polls the status of the UNI and all 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. **Note** The **t392** keyword is not supported when the router is in CE mode.
Step 7	`Router` **# end**	Return to privileged EXEC mode.
Step 8	`Router` **# show ethernet lmi evc**	Verify the configuration.
Step 9	`Router` **# 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.

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 the OAM manager on a PE device and on a CE device. You can configure the router as a PE device or CE device.

Provider-Edge Device Configuration

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

```
Router# config t
Router(config)# ethernet cfm domain Top level 7
Router(config)# ethernet cfm domain Provider level 4
Router(config-ether-cfm)# service customer_1 evc 101
Router(config-ether-cfm)# exit
Router(config)# ethernet cfm domain Operator_level 2
Router(config-ether-cfm)# service operator_1 evc 102
Router(config-ether-cfm)# exit
Router(config)# ethernet cfm enable
Router(config)# ethernet evc 101
Router(config-evc)# oam protocol cfm domain Provider
Router(config-evc)# exit
Router(config)# ethernet evc 102
Router(config-evc)# uni count 3
Router(config-evc)# oam protocol cfm domain Operator
Router(config-evc)# exit
Router(config)# ethernet lmi global
Router(config)# interface gigabitethernet 0
Router(config-if)# ethernet cfm mip level 7
Router(config-if)# service instance 101 ethernet 101
Router(config-if-srv)# encapsulation dot1q 101
Router(config-if-srv)# ethernet lmi ce-vlan map 101
Router(config-if-srv)# bridge-domain 101
Router(config-if-srv)# cfm mep domain Provider mpid 200
Router(config-if-srv)# exit
Router(config-if)# service instance 102 ethernet 102
Router(config-if-srv)# encapsulation dot1q 102
Router(config-if-srv)# ethernet lmi ce-vlan map 102
Router(config-if-srv)# bridge-domain 102
Router(config-if-srv)# cfm mep domain Operator mpid 201
Router(config-if-srv)# exit
Router(config-if)# exit
Router(config)# ethernet cfm cc enable level 4 evc 101
Router(config)# ethernet cfm cc enable level 2 evc 102
Router(config)# exit
```

Customer-Edge Device Configuration

This example shows the commands necessary to configure E-LMI on the CE device. Devices such as Cisco 3750-ME 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.

```
Router# config t
Router(config)# ethernet lmi global
Router(config)# ethernet lmi ce
Router(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 **routerport 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 34-3 to display E-LMI or OAM manager information.

Table 34-3 Displaying E-LMI and OAM Manager Information

Command	Purpose
show ethernet lmi evc [**detail** *evc-id* [**interface** *interface-id*] | **map interface** *type number*]	Displays details sent to the CE from the status request poll about the E-LMI EVC.
show ethernet lmi parameters interface *interface-id*	Displays Ethernet LMI interface parameters sent to the CE from the status request poll.
show ethernet lmi statistics interface *interface-id*	Displays Ethernet LMI interface statistics sent to the CE from the status request poll.
show ethernet lmi uni map interface [*interface-id*]	Displays information about the E-LMI UNI VLAN map sent to the CE from the status request poll.
show ethernet service evc {**detail | id** *evc-id* | **interface** *interface-id*}	Displays information about the specified EVC 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 EFPs.
show ethernet service interface [*interface-id*] [**detail**]	Displays information about the OAM manager interfaces.

Ethernet CFM and Ethernet OAM Interaction

To understand how CFM and OAM interact, you should understand the following concepts:

- Ethernet Virtual Circuit, page 34-43
- OAM Manager, page 34-43
- Configuring Ethernet OAM Interaction with CFM, page 34-44
- Ethernet OAM and CFM Configuration Example, page 34-45

Ethernet Virtual Circuit

An EVC as defined by the Metro Ethernet Forum is a port-level point-to-point or multipoint-to-multipoint Layer 2 circuit. EVC status can be used by a CE device either to find an alternative path in to the service provider network or in some cases, to fall back to a backup path over Ethernet or over another alternative service such as Frame Relay (FM) or Asynchronous Transmission Mode (ATM).

OAM Manager

The OAM manager is an infrastructure element that streamlines interaction between OAM protocols. The OAM manager requires two interworking OAM protocols, in this case Ethernet CFM and Ethernet OAM. Interaction is unidirectional from the OAM manager to the CFM protocol and the only information exchanged is the UNI port status. Additional port status values for the IEEE 802.3ah events with ML-MR-10 card include:

- REMOTE_EE—Remote excessive errors are reported through the CFM CC messages when IEEE 802.3ah peer reports errors.
- LOCAL_EE—Local excessive errors are reported through the CFM CC messages when local errors are found by IEEE 802.3ah.
- ADMINDOWN- Status is reported through the CFM CC messages when the interface on which 802.3ah is running is administratively shut down.
- DOWN- status is reported when the IEEE 802.3ah peer is not reachable.
- UP- status is reported when no errors found by 802.3ah.
- TEST- status is reported when either remote or local loopback is initiated.

After CFM receives the port status, it communicates that status across the CFM domain.

You can 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.

Table 34-4 CFM Response for Ethernet OAM Protocol Notifications/Conditions

Event	CFM Response
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.

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

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

Configuring Ethernet OAM Interaction with CFM

For Ethernet OAM to function with CFM, you must configure an 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.

Note You can configure an interface as Active or Passive on the ML-MR-10 card. If the interface is in passive state, the module replies only to the 802.3ah packets.

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	`Router # configure terminal`	Enter global configuration mode.
Step 2	`Router # 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	`Router # service csi-id evc evc_id`	Define a universally unique customer service instance (CSI) and EVC ID within the maintenance domain. • *csi-id*—String of no more than 100 characters that identifies the CSI. • *evc-id*- String of no more than 100 characters that identify a service. You cannot use the same *evc-id* for more than one domain at the same level.
Step 4	`Router # exit`	Return to global configuration mode.
Step 5	`Router # ethernet evc evc-id`	Define an EVC, and enter EVC configuration mode
Step 6	`Router # oam protocol cfm domain domain-name`	Configure the EVC OAM protocol as CFM, and identify 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.
Step 7	`Router # exit`	Return to global configuration mode.

	Command	Purpose
Step 8	Repeat Step 2 through Step 7 to define other CFM domains that you want the OAM manager to monitor.	
Step 9	`Router` **# ethernet cfm enable**	Globally enable CFM.
Step 10	`Router` **# end**	Return to privileged EXEC mode.
Step 11	`Router` **# 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	Router # **configure terminal**	Enter global configuration mode.
Step 2	Router # **interface** *interface-id*	Define an interface to configure as an Ethernet OAM interface and enter interface configuration mode.
Step 3	Router # **ethernet oam** [**max-rate** *oampdus* | **min-rate** *seconds* | **mode** {**active** | **passive**} | **timeout** *seconds*]	Enable Ethernet OAM on the interface • (Optional) Enter **max-rate** *oampdus t*o 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	Router # **end**	Return to privileged EXEC mode.
Step 5	Router # **copy running-config startup-config**	(Optional) Save your entries in the configuration file.
Step 6	Router # **show ethernet cfm maintenance points remote**	(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 PE router connected to a CE router at each endpoint. You must configure CFM, E-LMI, and Ethernet OAM between the CE and the PE router.

Customer-edge router 1 (CE1) configuration:

```
Router# config t
Router(config)# interface gigabitethernet0
Router(config-if)# ethernet oam remote-loopback supported
Router(config-if)# ethernet oam
Router(config-if)# service instance 10 ethernet BLUE
Router(config-if-srv)# encapsulation dot1q 10
Router(config-if-srv)# bridge-domain 10
Router(config-if)# exit
```

Provider-edge router 1 (PE1) configuration:

```
Router# config t
Router(config)# ethernet cfm domain TopMost level 7
Router(config)# ethernet cfm domain OperatorA level 1
Router(config-ether-cfm)# service CustomerX evc BLUE
Router(config)# ethernet evc BLUE
Router(config-evc)# oam protocol cfm domain OperatorA
Router(config)# interface gigabitethernet0
Router(config-if)# ethernet cfm mip level 7
Router(config-if)# ethernet uni id PE1
Router(config-if)# ethernet oam remote-loopback supported
Router(config-if)# ethernet oam
Router(config-if)# service instance 10 ethernet BLUE
Router(config-if-srv)# encapsulation dot1q 10
Router(config-if-srv)# cfm mep domain OperatorA inward mpid 21
Router(config-if-srv)# bridge-domain 10
Router(config-if-srv)# ethernet lmi ce-vlan map 10
Router(config-if-srv)# exit
```

Provider-edge router 2 (PE2) configuration:

```
Router# config t
Router(config)# ethernet cfm domain TopMost level 7
Router(config)# ethernet cfm domain OperatorA level 1
Router(config-ether-cfm)# service CustomerX evc BLUE
Router(config)# ethernet evc BLUE
Router(config-evc)# oam protocol cfm domain OperatorA
Router(config)# interface gigabitethernet0
Router(config-if)# ethernet cfm mip level 7
Router(config-if)# ethernet uni id PE2
Router(config-if)# ethernet oam remote-loopback supported
Router(config-if)# ethernet oam
Router(config-if)# service instance 10 ethernet BLUE
Router(config-if-srv)# encapsulation dot1q 10
Router(config-if-srv)# cfm mep domain OperatorA inward mpid 22
Router(config-if-srv)# bridge-domain 10
Router(config-if-srv)# ethernet lmi ce-vlan map 10
Router(config-if-srv)# exit
```

Customer-edge router 2 (CE2) configuration:

```
Router# config t
Router(config)# interface gigabitethernet0
Router(config-if)# ethernet oam remote-loopback supported
Router(config-if)# ethernet oam
Router(config-if)# service instance 10 ethernet BLUE
Router(config-if-srv)# encapsulation dot1q 10
Router(config-if-srv)# bridge-domain 10
Router(config-if)# exit
```

These are examples of the output showing provider-edge router port status of the configuration. Port status shows as UP at both routers.

Router PE1:

```
Router# show ethernet cfm maintenance points remote
Router PE1:
MPID  Level Mac Address    PortState InGressPort  Age(sec) Service ID  EVC
22  * 1     0019.076c.7dcd UP        Gi6          11       CustomerX  BLUE
```

Router PE2:

```
Router# show ethernet cfm maintenance points remote
MPID  Level Mac Address    PortState InGressPort  Age(sec) Service ID  EVC
21  * 1     0012.00a3.3780 UP        Gi6          8        CustomerX   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 router shows as Test and the remote CE router goes into error-disable mode.

```
Router# ethernet oam remote-loopback start interface gigabitEthernet 0
```

Router PE1:

```
Router# show ethernet cfm maintenance points remote
MPID  Level Mac Address    PortState InGressPort  Age(sec) Service ID  EVC
22  * 1     0019.076c.7dcd UP        Gi6          11       CustomerX   BLUE
```

Router PE2:

```
Router# show ethernet cfm maintenance points remote
MPID  Level Mac Address    PortState InGressPort  Age(sec) Service ID  EVC
21  * 1     0012.00a3.3780 TESR      Gi6          8        CustomerX   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.