CHAPTER 46

Configuring Ethernet CFM

The Catalyst 4500 series switch supports Standardized (Draft 8.1) IEEE 802.1ag Connectivity Fault Management (CFM) and IEEE 802.3ah Ethernet OAM discovery, link monitoring, remote fault detection, and remote loopback. It also supports IP Service Level Agreements (SLAs) for CFM, and ITU-T Y.1731 fault management.

This chapter provides information about configuring CFM and includes configuration information for CFM ITU-TY.1731 fault management support.

For complete command and configuration information for CFM and Y.1731, see the Cisco IOS Carrier Ethernet Configuration Guide at this URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/cether/configuration/15-mt/ce-15-mt-book.html

For complete syntax of the commands used in this chapter, see the command reference for this release and the Cisco IOS Carrier Ethernet Command Reference at this URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/cether/command/ce-cr-book.html

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

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

This chapter contains these sections:

About Ethernet CFM

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

These sections contain conceptual information about Ethernet CFM:

Ethernet CFM and OAM Definitions

The following table describes many of the terms in this chapter that are related to OAM and CFM features:

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

CFM Domain

A CFM maintenance domain is a management space on a network that is owned and operated by a single entity and defined by a set of internal boundary ports. You assign a unique maintenance level (from 0 to 7) to define the domain hierarchy. The larger the domain, the higher the level. For example, as shown in Figure 46-1, a service-provider domain would be larger than an operator domain and might have a maintenance level of 6, while the operator domain maintenance level would be 3 or 4.

As shown in Figure 46-2, domains cannot intersect or overlap because that would require management by more than one entity, which is not allowed. Domains can touch or nest (if the outer domain has a higher maintenance level than the nested domain). Nesting domains can be useful when a service provider contracts with one or more operators to provide Ethernet service. Each operator has its own maintenance domain and the service provider domain is a superset of the operator domains. Maintenance levels of nesting domains should be communicated among the administrating organizations. CFM exchanges messages and performs operations on a per-domain basis.

Figure 46-1 CFM Maintenance Domains

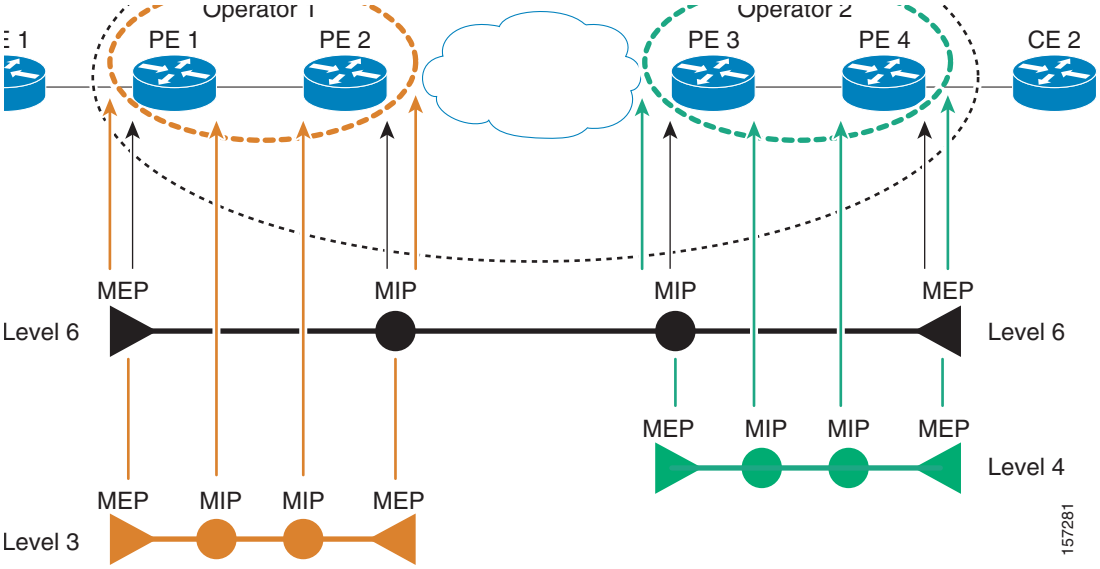
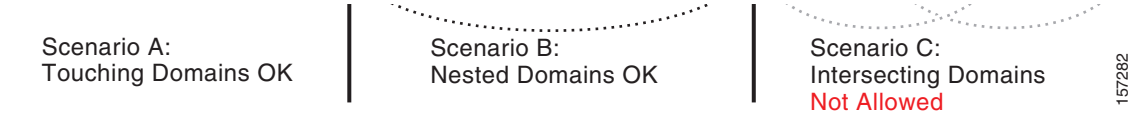


Figure 46-2 Allowed Domain Relationships



Maintenance Associations and Maintenance Points

A maintenance association (MA) identifies a service that can be uniquely identified within the maintenance domain. The CFM protocol runs within a maintenance association.A maintenance point is a demarcation point on an interface that participates in CFM within a maintenance domain. Maintenance points drop all lower-level frames and forward all higher-level frames. There are two types of maintenance points:

- Maintenance end points (MEPs) are points at the edge of the domain that define the boundaries and confine CFM messages within these boundaries. Down MEPs communicate through the wire side (connected to the port). Up MEPs communicate through the relay function side, not the wire side.

  CFM 802.1ag supports up and down per-VLAN MEPs, as well as port MEPs, which are untagged down MEPs that are not associated with a VLAN. Port MEPs are configured to protect a single hop and used to monitor link state through CFM. If a port MEP is not receiving continuity check

messages from its peer (static remote MEP), for a specified interval, the port is put into an operational down state in which only CFM and OAM packets pass through, and all other data and control packets are dropped.

  - An up MEP sends and receives CFM frames through the relay function. It drops all CFM frames at its level or lower that come from the wire side, except traffic going to the down MEP. 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. If the port on which MEP is configured is blocked by STP, the MEP can still send or receive CFM messages through the relay function. CFM runs at the provider maintenance level (UPE-to-UPE), specifically with up MEPs at the user network interface (UNI).
  - A down MEP sends and receives CFM frames through the wire connected to the port on which the MEP is configured. It drops all CFM frames at its level or lower that come from the relay side. For CFM frames from the wire side, it processes all CFM frames at its level and drops CFM frames at lower levels except traffic going to the other lower-level down MEP. The MEP transparently forwards all CFM frames at a higher level, regardless of whether they are received from the relay or through the wire

- 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 (unless MIP filtering is enabled), and forward all CFM frames at a higher level and at a lower level and regardless of whether they are received from the relay or wire side. When MIP filtering is enabled, the MIP drops CFM frames at a lower level. MIPs also catalog and forward continuity check messages (CCMs), but do not respond to them.

In draft 8.1, MIP filtering is disabled by default, and you can configure it to be enabled or disabled. When MIP filtering is disabled, all CFM frames are forwarded.

You can manually configure a MIP or configure the switch to automatically create a MIP. You can configure a MEP without a MIP. In case of a configuration conflict, manually created MIPs take precedence over automatically created MIPs.

If port on which the MEP is configured is blocked by Spanning-Tree Protocol (STP), the MIP can receive and might respond to CFM messages from both the wire and relay side, but cannot forward any CFM messages.

CFM Messages

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

- **Continuity Check (CC) messages**—multicast heartbeat messages exchanged periodically between MEPs that allow MEPs to discover other MEPs within a domain and allow MIPs to discover MEPs. CC messages are configured to a domain or VLAN. Enter the **continuity-check Ethernet service** configuration command to enable CCM.

  The default continuity check message (CCM) interval on the switch is 10 seconds. You can set it to be 100 ms, 1 second, 1 minute, or 10 minutes by entering the **continuity-check interval Ethernet service mode** command. Because faster CCM rates are more CPU intensive, we do not recommend configuring a large number of MEPs running at 100 ms intervals.

- **Loopback messages**—unicast or multicast frames transmitted by a MEP at administrator request to verify connectivity to a particular maintenance point, indicating if a destination is reachable. A loopback message is similar to an Internet Control Message Protocol (ICMP) ping message. Refer to the **ping ethernet** privileged EXEC command.
- **Traceroute messages**—multicast frames transmitted by a MEP at administrator request to track the path (hop-by-hop) to a destination MEP. Traceroute messages are similar in concept to UDP traceroute messages. Refer to the **traceroute ethernet** privileged EXEC command.

Crosscheck Function and Static Remote MEPs

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

CFM 802.1ag also supports static remote MEPs or static RMEP check. Unlike the crosscheck function, which is performed only once, configured static RMEP checks run continuously. To configure static RMEP check, enter the **continuity-check static rmep** Ethernet CFM service mode command.

SNMP Traps and Fault Alarms

The MEPs generate two types of SNMP traps: CC traps and crosscheck traps. Supported CC traps are MEP up, MEP down, cross-connect (a service ID does not match the VLAN), loop, and configuration error. The crosscheck traps are service up, MEP missing (an expected MEP is down), and unknown MEP.

Fault alarms are unsolicited notifications sent to alert the system administrator when CFM detects a fault. In CFM 802.1ag, you can configure the priority level of alarms that trigger an SNMP trap or syslog message. You can also configure a delay period before a fault alarm is sent and the time before the alarm is reset.

Configuration Error List

CFM configuration errors in CFM 802.1ag can be misconfigurations or extra configuration commands detected during MEP configuration. They can be caused by overlapping maintenance associations. For example, if you create a maintenance association with a VLAN list and a MEP on an interface, a potential leak error could occur if other maintenance associations associated with the same VLAN exist at a higher level without any MEPs configured. You can display the configuration error list, which is informational only, by entering the **show ethernet cfm errors** configuration privileged EXEC command.

IP SLAs Support for CFM

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

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

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

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

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

Configuring Ethernet CFM

CFM draft 8.1 on Catalyst 4500 series switch mandates that you enter the **ethernet cfm ieee** command before configuring any other CFM CLI. Without this command, no other CFM CLIs are applied. Configuring Ethernet CFM requires that you configure the CFM domain. You can optionally configure and enable other CFM features (such as crosschecking, static remote MEP, port MEPs, CVLAN MEPs/MIPs, SNMP traps, and fault alarms).

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

Ethernet CFM Default Configuration

CFM is globally disabled.

CFM is enabled on all interfaces when CFM is globally enabled.

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

There are no MEPs or MIPs configured.

When configuring a MA, if you do not configure direction, the default is up (inward facing).

Ethernet CFM Configuration Guidelines

When configuring Ethernet CFM, consider these guidelines and restrictions:

- You must enter the **ethernet cfm ieee** global configuration command before configuring any other CFM CLI. If not, all other CFM CLIs are not applied.
- CFM is not supported on and cannot be configured on either routed ports or Layer 3 EtherChannels.
- You can configure a Layer 2 EtherChannel port channel as Up MEP, Down MEP, or MIP. However, such configurations are not supported on individual ports that belong to an EtherChannel. You cannot add a port with this configuration to an EtherChannel group.
- Port MEP is not supported and cannot be configured on Layer 2 EtherChannels.
- CFM is not supported and cannot be configured on VLAN interfaces.
- On isolated host, community host, or a promiscuous access port, only Down MEP is supported on isolated, community and primary VLANs, respectively.
- Up MEP is supported only on regular VLANs on PVLAN trunks. Down MEP is supported on regular VLANs as well as isolated VLANs on PVLAN secondary trunks. Similarly, Down MEP is supported on regular VLANs as well as primary VLANs on promiscuous trunk ports.
- The CFM service on a PVLAN ends at the PVLAN port. The translation of CFM service between PVLANs is not supported between the PVLAN ports.
- CFM Unicast packets (Loopback Messages and Traceroute Reply), are not allowed on Down MEP on STP blocked ports. The blocked port cannot respond to ping and traceroute. You must configure a port MEP at a lower level than any service (VLAN) MEPs on an interface.
- An 802.1Q (QinQ) tunnel port can be an Up MEP or a port MEP.
- A QinQ port cannot be a Down MEP or a MIP; you can configure the port as a MIP, but it is not active or visible in traceroute. Port MEP frames received on a QinQ interface are not tunneled and are processed locally.
- CFM on a C-VLAN is supported on Traditional and Selective QinQ and not supported on One-to-One VLAN Mapping on Trunk ports.
- Do not configure a port with tunnel mode using the native VLAN as the S-VLAN or the C-VLAN.
- For port MEP on a QinQ port, do not enter the **vlan dot1q tag native** global configuration command to enable tagging on native VLAN frames.

Configuring the CFM Domain

To configure the Ethernet CFM domain, configure a service to connect the domain to a VLAN, or configure a port to act as a MEP, perform this task. You can also enter the optional commands to configure other parameters, such as continuity checks.

	Command	Purpose
Step 1	`configure terminal`	Enter global configuration mode.
Step 2	`ethernet cfm ieee`	A must have configuration for draft 8.1. This is required to be configured before any other configuration.
Step 3	`ethernet cfm global`	Globally enable Ethernet CFM on the switch.

	Command	Purpose
Step 4	**ethernet cfm traceroute cache** [**size** *entries* | **hold-time** *minutes*]	(Optional) Configure the CFM traceroute cache. You can set a maximum cache size or hold time. • (Optional) For **size**, enter the cache size in number of entry lines. The range is from 1 to 4095; the default is 100 lines. • (Optional) For **hold-time**, enter the maximum cache hold time in minutes. The range is from 1 to 65535; the default is 100 minutes.
Step 5	**ethernet cfm mip auto-create level** *level-id* **vlan** *vlan-id*	(Optional) Configure the switch to automatically create MIPs for VLAN IDS that are not associated with specific maintenance associations at the specified level. The level range is 0 to 7. **Note** Configure MIP auto-creation only for VLANs that MIPs should monitor. Configuring for all VLANs can be CPU and memory-intensive.
Step 6	**ethernet cfm mip filter**	(Optional) Enable MIP filtering, which means that all CFM frames at a lower level are dropped. The default is disabled.
Step 7	**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 8	**id** {*mac-address domain_number* | **dns** *name* | **null**}	(Optional) Assign a maintenance domain identifier. • *mac-address domain_number*—Enter the MAC address and a domain number. The number can be from 0 to 65535. • **dns** *name*—Enter a DNS name string. The name can be a maximum of 43 characters. • **null**—Assign no domain name.
Step 9	**service** {*ma-name* | *ma-number* | *vpn-id vpn*} {**vlan** *vlan-id* [**direction down**] | **port**}	Define a customer service maintenance association (MA) name or number or VPN ID to be associated with the domain, a VLAN ID or port MEP, and enter ethernet-cfm-service configuration mode. • *ma-name*—a string of no more than 100 characters that identifies the MAID. • *ma-number*—a value from 0 to 65535. • *vpn-id vpn*—enter a VPN ID as the *ma-name*. • **vlan** *vlan-id*—VLAN range is from 1 to 4094. You cannot use the same VLAN ID for more than one domain at the same level. • (Optional) **direction down**—specify the service direction as down. • **port**—Configure port MEP, a down MEP that is untagged and not associated with a VLAN.
Step 10	**continuity-check**	Enable sending and receiving of continuity check messages.

	Command	Purpose
Step 11	**continuity-check interval** *value*	(Optional) Set the interval at which continuity check messages are sent. The available values are 100 ms, 1 second, 10 seconds, 1 minute and 10 minutes. The default is 10 seconds. **Note** Because faster CCM rates are more CPU-intensive, we do not recommend configuring a large number of MEPs running at 100 ms intervals.
Step 12	**continuity-check loss-threshold** *threshold-value*	(Optional) Set the number of continuity check messages to be missed before declaring that an MEP is down. The range is 2 to 255; the default is 3.
Step 13	**maximum meps** *value*	(Optional) Configure the maximum number of MEPs allowed across the network. The range is from 1 to 65535. The default is 100.
Step 14	**sender-id** {**chassis** | **none**}	(Optional) Include the sender ID TLVs, attributes containing type, length, and values for neighbor devices. • **chassis**—Send the chassis ID (host name). • **none**—Do not include information in the sender ID.
Step 15	**mip auto-create** [**lower-mep-only** | **none**]	(Optional) Configure auto creation of MIPs for the service. • **lower-mep-only**—Create a MIP only if there is a MEP for the service in another domain at the next lower active level. • **none** —No MIP auto-create.
Step 16	**exit**	Return to ethernet-cfm configuration mode.
Step 17	**mip auto-create** [**lower-mep-only**]	(Optional) Configure auto creation of MIPs for the domain. • **lower-mep-only**—Create a MIP only if there is a MEP for the service in another domain at the next lower active level.
Step 18	**mep archive-hold-time** *minutes*	(Optional) Set the number of minutes that data from a missing maintenance end point is kept before it is purged. The range is 1 to 65535; the default is 100 minutes.
Step 19	**exit**	Return to global configuration mode.
Step 20	**interface** *interface-id*	Specify an interface to configure, and enter interface configuration mode.
Step 21	**switchport mode trunk**	(Optional) Configure the port as a trunk port.
Step 22	**ethernet cfm mip level** *level-id*	(Optional) Configure a customer level or service-provider level maintenance intermediate point (MIP) for the interface. The MIP level range is 0 to 7. **Note** This step is not required if you have entered the **ethernet cfm mip auto-create** global configuration command or the **mip auto-create** ethernet-cfm or ethernet-cfm-srv configuration mode.

	Command	Purpose
Step 23	**ethernet cfm mep domain** *domain-name* **mpid** *identifier* {**vlan** *vlan-id* | **port**}	Configure maintenance end points for the domain, and enter ethernet cfm mep mode. • **domain** *domain-name*—Specify the name of the created domain. • **mpid** *identifier*—Enter a maintenance end point identifier. The identifier must be unique for each VLAN (service instance). The range is 1 to 8191. • **vlan** *vlan-id*—Enter the service provider VLAN ID or IDs as a VLAN-ID (1 to 4094), a range of VLAN-IDs separated by a hyphen, or a series of VLAN IDs separated by comma. • **port**—Configure port MEP.
Step 24	**cos** *value*	(Optional) Specify the class of service (CoS) value to be sent with the messages. The range is 0 to 7.
Step 25	**end**	Return to privileged EXEC mode.
Step 26	**show ethernet cfm maintenance-points** {**local** | **remote**}	Verify the configuration.
Step 27	**show ethernet cfm errors [configuration]**	(Optional) Display the configuration error list.
Step 28	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

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

This is an example of the basic CFM configuration:

```
Switch(config)# ethernet cfm ieee
Switch(config)# ethernet cfm global
Switch(config)# ethernet cfm domain abc level 3
Switch(config-ecfm)# service test vlan 5
Switch(config-ecfm-srv)# continuity-check
Switch(config-ecfm-srv)# exit
Switch(config-ecfm)# exit
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# ethernet cfm mep domain abc mpid 222 vlan 5
Switch(config-if-ecfm-mep)# exit
```

Configuring Ethernet CFM Crosscheck

To configure Ethernet CFM crosscheck, perform this task:

	Command	Purpose
Step 1	Switch# **configure terminal**	Enters global configuration mode.
Step 2	Switch(config)# **ethernet cfm mep crosscheck start-delay** *delay*	Configures the number of seconds that the device waits for remote MEPs to come up before the crosscheck is started. The range is 1 to 65535; the default is 30 seconds.
Step 3	Switch(config)# **ethernet cfm domain** *domain-name* **level** *level-id*	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.

	Command	Purpose
Step 4	`Switch(config)# service {ma-name | ma-number | vpn-id vpn} {vlan vlan-id}`	Define a customer service maintenance association name or number or VPN ID to be associated with the domain, and a VLAN ID, and enter ethernet-cfm-service configuration mode. • *ma-name*—A string of no more than 100 characters that identifies the MAID. • *ma-number*—A value from 0 to 65535. • *vpn-id vpn*—Enter a VPN ID as the ma-name. • *vlan vlan-id*—VLAN range is from 1 to 4094. You cannot use the same VLAN ID for more than one domain at the same level.
Step 5	`Switch(config-ether-cfm)# mep mpid identifier`	Define the MEP maintenance end point identifier in the domain and service. The range is 1 to 8191.
Step 6	`Switch(config)# end`	Returns to privileged EXEC mode.
Step 7	`Switch# ethernet cfm mep crosscheck {enable | disable} domain domain-name {vlan {vlan-id | any} | port}`	• Enable or disable CFM crosscheck for one or more VLANs or a port MEP in the domain. • **domain** *domain-name*—Specify the name of the created domain. • **vlan** {*vlan-id* | **any**}—Enter the service provider VLAN ID or IDs as a VLAN-ID (1 to 4094), a range of VLAN-IDs separated by a hyphen, or a series of VLAN IDs separated by comma. Enter any for any VLAN. • **port**—Identify a port MEP
Step 8	`Switch# show ethernet cfm maintenance-points remote crosscheck`	Verifies the configuration.
Step 9	`Switch# show ethernet cfm errors [configuration]`	Enter this command after you enable CFM crosscheck to display the results of the crosscheck operation. Enter the **configuration** keyword to display the configuration error list.
Step 10	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

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

The following example illustrates how to configure Ethernet CFM crosscheck:

```
Switch(config)# ethernet cfm mep crosscheck start-delay 60
Switch(config)# ethernet cfm domain abc level 3
Switch(config-ecfm)# service test vlan 5
Switch(config-ecfm-srv)# mep mpid 23
Switch(config-ecfm-srv)# mep mpid 34
Switch(config-ecfm-srv)# end
Switch# ethernet cfm mep crosscheck enable domain abc vlan 5

Switch# show ethernet cfm maintenance-points remote crosscheck
-------------------------------------------------------------------------------
MPID Domain Name                                Lvl Type Id       Mep-Up
     MA Name
-------------------------------------------------------------------------------
  23 abc                                          3 Vlan 5            No
```

```
     test
  34 abc                                          3 Vlan 5            No
     test

Switch# show ethernet cfm errors
----------------------------------------------------------------------------------
MPID Domain Id                                   Mac Address      Type Id
     MA Name                                     Reason           Lvl  Age
----------------------------------------------------------------------------------
34   abc                                         0000.0000.0000   Vlan 5
     test                                        RMEP missing     3    95s
23   abc                                         0000.0000.0000   Vlan 5
     test                                        RMEP missing     3    95s
Switch#
```

Configuring Static Remote MEP

To configure Ethernet CFM static remote MEP, perform this task:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ethernet cfm domain** *domain-name* **level** *level-id*	Define a CFM domain, set the domain level, and enter ethernet-cfm configuration mode for the domain. The maintenance level number range is 0 to 7.
Step 3	**service** {*ma-name* | *ma-number* | *vpn-id vpn*} {**vlan** *vlan-id* [**direction down**] | **port**}	Define a customer service maintenance association name or number or a VPN ID to be associated with the domain, and a VLAN ID or peer MEP, and enter ethernet-cfm-service configuration mode. • *ma-name*—a string of no more than 100 characters that identifies the MAID. • *ma-number*—a value from 0 to 65535. • *vpn-id*—enter a VPN ID as the *ma-name*. • **vlan** *vlan-id*—VLAN range is from 1 to 4094. You cannot use the same VLAN ID for more than one domain at the same level. • (Optional) **direction down**—specify the service direction as down. • **port**—Configure port MEP, a down MEP that is untagged and not associated with a VLAN.
Step 4	**continuity-check**	Enable sending and receiving of continuity check messages.
Step 5	**mep mpid** *identifier*	Define the static remote maintenance end point identifier. The range is 1 to 8191.
Step 6	**continuity-check static rmep**	Enable checking of the incoming continuity check message from a remote MEP that is configured in the MEP list.
Step 7	**end**	Return to privileged EXEC mode.
Step 8	**show ethernet cfm maintenance-points remote static**	Verify the configuration.

	Command	Purpose
Step 9	**show ethernet cfm errors** [**configuration**]	Enter this command after you enable CFM crosscheck to display the results of the crosscheck operation. Enter the **configuration** keyword to display the configuration error list.
Step 10	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

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

The following example illustrates how to configure Ethernet CFM static remote MEP:

```
Switch(config)# ethernet cfm domain abc level 3
Switch(config-ecfm)# service test vlan 5
Switch(config-ecfm-srv)# continuity-check
Switch(config-ecfm-srv)# mep mpid 23
Switch(config-ecfm-srv)# mep mpid 34
Switch(config-ecfm-srv)# continuity-check static rmep

Switch# show ethernet cfm maintenance-points remote static
-------------------------------------------------------------------------
MPID Domain Name                                Lvl Type Id       Mep-Up
     MA Name
-------------------------------------------------------------------------
  23 abc                                          3 Vlan 5            No
     test
  34 abc                                          3 Vlan 5            No
     test
Switch# show ethernet cfm errors
-------------------------------------------------------------------------------
MPID Domain Id                                  Mac Address      Type Id
     MA Name                                    Reason           Lvl  Age
-------------------------------------------------------------------------------
34   abc                                        0000.0000.0000   Vlan 5
     test                                       RMEP missing     3    421s
23   abc                                        0000.0000.0000   Vlan 5
     test                                       RMEP missing     3    421s
Switch#
```

Configuring a Port MEP

A port MEP is a down MEP that is not associated with a VLAN and that uses untagged frames to carry CFM messages. You configure port MEPs on two connected interfaces. Port MEPs are always configured at a lower domain level than native VLAN MEPs.

To configure Ethernet CFM port MEPs, perform this task:

	Command	Purpose
Step 1	Switch# **configure terminal**	Enters global configuration mode.
Step 2	Switch(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.

	Command	Purpose
Step 3	`Switch(config-ecfm)# service {ma-name | ma-number | vpn-id} port`	Defines a customer service maintenance association name or number or VPN ID to be associated with the domain, define a port MEP, and enter ethernet-cfm-service configuration mode. • *ma-name*—a string of no more than 100 characters that identifies the MAID. • *ma-number*—a value from 0 to 65535. • *vpn-id vpn*—enter a VPN ID as the *ma-name*.
Step 4	`Switch(config-ecfm-srv)# mep mpid identifier`	Defines the static remote maintenance end point identifier in the domain and service. The range is 1 to 8191.
Step 5	`Switch(config-ecfm-srv)# continuity-check`	Enables sending and receiving of continuity check messages.
Step 6	`Switch(config-ecfm-srv)# continuity-check interval value`	(Optional) Sets the interval at which continuity check messages are sent. The available values are 1 second, 10 seconds, 1 minute, and 10 minutes. The default is 10 seconds. **Note** Because faster CCM rates are more CPU-intensive, we do not recommend configuring a large number of MEPs running at 1 s intervals.
Step 7	`Switch(config-ecfm-srv)# continuity-check loss-threshold threshold-value`	(Optional) Sets the number of continuity check messages to be missed before declaring that an MEP is down. The range is 2 to 255; the default is 3.
Step 8	`Switch(config-ecfm-srv)# continuity-check static rmep`	Enables checking of the incoming continuity check message from a remote MEP that is configured in the MEP list.
Step 9	`Switch(config-ecfm-srv)# exit`	Returns to ethernet-cfm configuration mode.
Step 10	`Switch(config-ecfm)# exit`	Returns to global configuration mode.
Step 11	`Switch(config)# interface interface-id`	Identifies the port MEP interface and enter interface configuration mode.
Step 12	`Switch(config-if)# ethernet cfm mep domain domain-name mpid identifier port`	Configures the interface as a port MEP for the domain. • **domain** *domain-name*—Specify the name of the created domain. • **mpid** *identifier*—Enter a maintenance end point identifier. The identifier must be unique for each VLAN (service instance). The range is 1 to 8191.
Step 13	`Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 14	`Switch)# show ethernet cfm maintenance-points remote static`	Verifies the configuration.
Step 15	`Switch)# show ethernet cfm errors [configuration]`	Enters this command after you enable CFM crosscheck to display the results of the crosscheck operation. Enter the **configuration** keyword to display the configuration error list.
Step 16	`Switch)# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

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

This is a sample configuration for a port MEP:

```
Switch(config)# ethernet cfm domain abc level 3
Switch(config-ecfm)# service PORTMEP port
Switch(config-ecfm-srv)# mep mpid 222
Switch(config-ecfm-srv)# continuity-check
Switch(config-ecfm-srv)# continuity-check static rmep
Switch(config-ecfm-srv)# exit
Switch(config-ecfm)# exit
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ethernet cfm mep domain abc mpid 111 port
Switch(config-if)# end
```

Configuring SNMP Traps

To configure traps for Ethernet CFM, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# snmp-server enable traps ethernet cfm cc [mep-up] [mep-down] [config] [loop] [cross-connect]`	(Optional) Enables Ethernet CFM continuity check traps.
Step 3	`Switch(config)# snmp-server enable traps ethernet cfmalarm`	(Optional) Enables Ethernet CFM fault alarm trap.
Step 4	`Switch(config)# snmp-server enable traps ethernet cfm crosscheck [mep-unknown] [mep-missing] [service-up]`	(Optional) Enable s Ethernet CFM crosscheck traps.
Step 5	`Switch(config)# end`	Returns to privileged EXEC mode.
Step 6	`Switch# show running-config`	Verifies your entries.
Step 7	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

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

The following example illustrates how to configure SNMP traps:

```
Switch(config)# snmp-server enable traps ethernet cfm alarm
Switch(config)# snmp-server enable traps ethernet cfm cc mep-down
Switch(config)# snmp-server enable traps ethernet cfm crosscheck mep-missing
```

Configuring Fault Alarms

To configure Ethernet CFM fault alarms, perform this task.

Note You can configure fault alarms in either global configuration or Ethernet CFM interface MEP mode. When a conflict exists, the interface MEP mode configuration takes precedence.

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**ethernet cfm alarm notification** {**all** | **error-xcon** | **mac-remote-error-xcon** | **none** | **remote-error-xcon** | **xcon**}	Globally enables Ethernet CFM fault alarm notification for the specified defects: • **all**—report all defects. • **error-xcon**—Report only error and connection defects. • **mac-remote-error-xcon**—Report only MAC-address, remote, error, and connection defects. • **none**—Report no defects. • **remote-error-xcon**—Report only remote, error, and connection defects. • **xcon**—Report only connection defects.
Step 3	**ethernet cfm alarm delay** *value*	(Optional) Sets a delay period before a CFM fault alarm is sent. The range is 2500 to 10000 milliseconds (ms). The default is 2500 ms.
Step 4	**ethernet cfm alarm reset** *value*	(Optional) Specifies the time period before the CFM fault alarm is reset. The range is 2500 to 10000 milliseconds (ms). The default is 10000 ms.
Step 5	**ethernet cfm logging alarm ieee**	Configures the switch to generate system logging messages for the alarms.
Step 6	**interface** *interface-id*	(Optional) Specifies an interface to configure, and enter interface configuration mode.
Step 7	**ethernet cfm mep domain** *domain-name* **mpid** *identifier* **vlan** *vlan-id*	Configures maintenance end points for the domain, and enter ethernet cfm interface mep mode. • **domain** *domain-name*—Specify the name of the created domain. • **mpid** *identifier*—Enter a maintenance end point identifier. The identifier must be unique for each VLAN (service instance). The range is 1 to 8191. • **vlan** *vlan-id*—Enter the service provider VLAN ID or IDs as a VLAN-ID (1 to 4094), a range of VLAN-IDs separated by a hyphen, or a series of VLAN IDs separated by comma.
Step 8	**alarm notification** {**all** | **error-xcon** | **mac-remote-error-xcon** | **none** | **remote-error-xcon** | **xcon**}	(Optional) Enables Ethernet CFM fault alarm notification for the specified defects on the interface. **Note** The Ethernet CFM interface MEP alarm configuration takes precedence over the global configuration.
Step 9	**alarm** {**delay** *value* | **reset** *value*}	(Optional) Sets an alarm delay period or a reset period. **Note** The Ethernet CFM interface MEP alarm configuration takes precedence over the global configuration.

	Command	Purpose
Step 10	`end`	Returns to privileged EXEC mode.
Step 11	`show running-config`	Verifies your entries.
Step 12	`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.

The following example illustrates how to configure Ethernet CFM fault alarms:

```
Switch(config)# ethernet cfm alarm notification remote-error-xcon
Switch(config)# ethernet cfm logging alarm ieee
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# ethernet cfm mep domain abc mpid 222 vlan 5
Switch(config-if-ecfm-mep)# alarm notification mac-remote-error-xcon
Switch(config-if)# end
```

Configuring IP SLAs CFM Operation

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

For detailed information about configuring IP SLAs Ethernet operations, see the *Cisco IOS IP SLAs for Metro-Ethernet* feature module at this URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/ipsla/configuration/15-1s/Configuring_Cisco_IOS_IP_SLAs_for_Metro-Ethernet.html

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

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

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

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

This section includes these procedures:

- Manually Configuring an IP SLAs CFM Probe or Jitter Operation, page 46-18
- Configuring an IP SLAs Operation with Endpoint Discovery, page 46-20

Manually Configuring an IP SLAs CFM Probe or Jitter Operation

To manually configure an IP SLAs Ethernet echo (ping) or jitter operation, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# ip sla operation-number`	Creates an IP SLAs operation, and enters IP SLAs configuration mode.

Step 3	`Switch(config-ip-sla)# ethernet echo mpid identifier domain domain-name vlan vlan-id`
	
	or
	
	`ethernet jitter mpid identifier domain domain-name vlan vlan-id [interval interpacket-interval] [num-frames number-of frames transmitted]`
		Configures the IP SLAs operation as an echo (ping) or jitter operation, and enter IP SLAs Ethernet echo configuration mode.
		• Enter **echo** for a ping operation or **jitter** for a jitter operation.
		• For **mpid** *identifier*, enter a maintenance endpoint identifier. The identifier must be unique for each VLAN (service instance). The range is 1 to 8191.
		• For **domain** *domain-name*, enter the CFM domain name.
		• For **vlan** *vlan-id*, the VLAN range is from 1 to 4095.
		• (Optional—for jitter only) Enter the **interval** between sending of jitter packets.
		• (Optional—for jitter only) Enter the **num-frames** and the number of frames to be sent.

Step 4	`Switch(config-ip-sla-ethernet-monitor)# cos cos-value`	(Optional) Sets a class of service value for the operation. Before configuring the **cos** parameter on the switch, you must globally enable QoS by entering the **mls qos** global configuration command.
Step 5	`Switch(config-ip-sla-ethernet-monitor)# frequency seconds`	(Optional) Sets the rate at which the IP SLAs operation repeats. The range is from 1 to 604800 seconds; the default is 60 seconds.
Step 6	`Switch(config-ip-sla-ethernet-monitor)# history history-parameter`	(Optional) Specifies parameters for gathering statistical history information for the IP SLAs operation.
Step 7	`Switch(config-ip-sla-ethernet-monitor)# owner owner-id`	(Optional) Configures the SNMP owner of the IP SLAs operation.
Step 8	`Switch(config-ip-sla-ethernet-monitor)# request-data-size bytes`	(Optional) Specifies the protocol data size for an IP SLAs request packet. The range is from 0 to the maximum size allowed by the protocol being used; the default is 66 bytes.
Step 9	`Switch(config-ip-sla-ethernet-monitor)# tag text`	(Optional) Creates user-specified identifier for an IP SLAs operation.
Step 10	`Switch(config-ip-sla-ethernet-monitor)# threshold milliseconds`	(Optional) Specifies the upper threshold value in milliseconds (ms) for calculating network monitoring statistics. The range is 0 to 2147483647; the default is 5000.

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

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

The following example illustrates how to configurean IP SLA CFM Probe or Jitter Operation:

```
Switch(config)# ip sla 1
Switch(config-ip-sla)# ethernet echo mpid 23 domain abc vlan 5
Switch(config-ip-sla-ethernet-echo)# exit
Switch(config)# ip sla schedule 1 start-time now

Switch# show ip sla configuration 1
IP SLAs, Infrastructure Engine-II.

Entry number: 1
Owner:
Tag:
Type of operation to perform: 802.1ag Echo
```

```
Target domain: abc
Target MPID: 23
Target VLAN ID: 5
Request size (Padding portion): 0
Operation timeout (milliseconds): 5000
Class Of Service parameters: 0
Schedule:
    Operation frequency (seconds): 60
    Next Scheduled Start Time: Start Time already passed
    Group Scheduled : FALSE
    Randomly Scheduled : FALSE
    Life (seconds): 3600
    Entry Ageout (seconds): never
    Recurring (Starting Everyday): FALSE
    Status of entry (SNMP RowStatus): Active
Threshold (milliseconds): 5000
Distribution Statistics:
    Number of statistic hours kept: 2
    Number of statistic distribution buckets kept: 1
    Statistic distribution interval (milliseconds): 20
Enhanced History:
History Statistics:
    Number of history Lives kept: 0
    Number of history Buckets kept: 15
    History Filter Type: None


Switch#
```

Configuring an IP SLAs Operation with Endpoint Discovery

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

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# ip sla ethernet-monitor` *operation-number*	Begins configuration of an IP SLAs automatic Ethernet operation, and enter IP SLAs Ethernet monitor configuration mode.

	Command	Purpose

Step 3	`Switch(config-ip-sla-ethernet-monitor)# type echo domain domain-name vlan vlan-id [exclude-mpids mp-ids]`
	
	or
	
	`type jitter domain domain-name vlan vlan-id [exclude-mpids mp-ids] [interval interpacket-interval] [num-frames number-of frames transmitted]`
		Configures the automatic Ethernet operation to create echo (ping) or jitter operation and enters IP SLAs Ethernet echo configuration mode.
		• Enter **type echo** for a ping operation or **type jitter** for a jitter operation.
		• For **mpid** *identifier*, enter a maintenance endpoint identifier. The range is 1 to 8191.
		• For **domain** *domain-name*, enter the CFM domain name.
		• For **vlan** *vlan-id*, the VLAN range is from 1 to 4095.
		• (Optional) Enter **exclude-mpids** *mp-ids* to exclude the specified maintenance endpoint identifiers.
		• (Optional—for jitter only) Enter the **interval** between sending of jitter packets.
		• (Optional—for jitter only) Enter the **num-frames** and the number of frames to be sent.

Step 4	`Switch(config-ip-sla-ethernet-echo)# cos cos-value`	(Optional) Sets a class of service value for the operation.
Step 5	`Switch(config-ip-sla-ethernet-echo)# owner owner-id`	(Optional) Configures the SNMP owner of the IP SLAs operation.
Step 6	`Switch(config-ip-sla-ethernet-echo)# request-data-size bytes`	(Optional) Specifies the protocol data size for an IP SLAs request packet. The range is from 0 to the maximum size allowed by the protocol being used; the default is 66 bytes.
Step 7	`Switch(config-ip-sla-ethernet-echo)# tag text`	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 8	`Switch(config-ip-sla-ethernet-echo)# threshold milliseconds`	(Optional) Specifies the upper threshold value in milliseconds for calculating network monitoring statistics. The range is 0 to 2147483647; the default is 5000.
Step 9	`Switch(config-ip-sla-ethernet-echo)# timeout milliseconds`	(Optional) Specifies the amount of time in milliseconds that the IP SLAs operation waits for a response from its request packet. The range is 0 to 604800000; the default value is 5000.
Step 10	`Switch(config-ip-sla-ethernet-echo)# exit`	Returns to global configuration mode.

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

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

The following example illustrates how to configurean an IP SLAs Operation with Endpoint Discovery:

```
Switch(config)# ip sla ethernet-monitor 10
Switch(config- ip-sla-ethernet-monitor)#type echo domain abc vlan 34
Switch(config-ip-sla-ethernet-params)# exit
Switch(config)# ip sla ethernet-monitor schedule 10 schedule-period 60 start-time now
Switch(config)# exit

Switch# show ip sla ethernet-monitor configuration 10
Entry Number : 10
Modification time   : *10:12:01.725 UTC Mon Nov 29 2010
Operation Type      : echo
Domain Name         : abc
VLAN ID             : 5
Excluded MPIDs      :
Owner               :
Tag                 :
Timeout(ms)         : 5000
Threshold(ms)       : 5000
Frequency(sec)      : 60
```

```
Operations List     : Empty
Schedule Period(sec): 60
Request size        : 0
CoS                 : 0
Start Time          : Start Time already passed
SNMP RowStatus      : Active


Switch#
```

Configuring CFM on C-VLAN (Inner VLAN)

IEEE 802.1ag CFM brings in a support that allows customers to provision maintenance intermediate points (MIPs) and Up maintenance endpoints (MEPs) on the C-VLAN (inner VLAN) component of QinQ ports to provide visibility on the C-VLAN. C-VLANs are now supported on 802.1q tunnel ports. This allows monitoring or troubleshooting when QinQ is enabled on the provider edge (PE) device.

For more information about this feature and the supported commands, see:

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

The switch supports 802.1q-tunnel-port mode.

To configure Ethernet CFM CVLAN Up MEPs, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# 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	`Switch(config-ecfm)# service` {*ma-name* | *ma-number* | *vpn-id*} `vlan` *svlan-id* `inner-vlan` *cvlan-id*	Define a customer service maintenance association name or number or VPN ID to be associated with the domain, define a CVLAN service, and enter ethernet-cfm-service configuration mode. • *ma-name*—a string of no more than 100 characters that identifies the MAID. • *ma-number*—a value from 0 to 65535. • *vpn-id vpn*—enter a VPN ID as the ma-name. • **vlan** *svlan-id*—VLAN range is from 1 to 4094. This identifies the outer VLAN (service provider VLAN ID) that CFM frames go out with. • **inner-vlan** *cvlan-id*—VLAN range is from 1 to 4094. This identifies the inner VLAN (customer VLAN) that is monitored through CFM.
Step 4	`Switch(config-ecfm-arv)# continuity-check`	Enables sending and receiving of continuity check messages.

	Command	Purpose
Step 5	`Switch(config-ecfm-arv)# continuity-check interval value`	(Optional) Set the interval at which continuity check messages are sent. The available values are 1 second, 10 seconds, 1 minute and 10 minutes. The default is 10 seconds. **Note** Because faster CCM rates are more CPU-intensive, we do not recommend configuring a large number of MEPs running at 1 s intervals.
Step 6	`Switch(config-ecfm-arv)# continuity-check loss-threshold threshold-value`	(Optional) Set the number of continuity check messages to be missed before declaring that an MEP is down. The range is 2 to 255; the default is 3.
Step 7	`Switch(config-ecfm-arv)# exit`	Returns to Return to ethernet-cfm configuration mode.
Step 8	`Switch(config-ecfm)# exit`	Returns to global configuration mode.
Step 9	`Switch(config)# interface interface-id`	Identify the CVLAN MEP interface and enter interface configuration mode.
Step 10	`Switch(config-if)# ethernet cfm mep domain domain-name mpid identifier service {ma-name | ma-number | vpn-id}]`	Configure the interface as a CVLAN Up MEP for the domain. • **domain** *domain-name*—Specify the name of the created domain. • **mpid** *identifier*—Enter a maintenance end point identifier. The identifier must be unique for each VLAN (service instance). The range is 1 to 8191. • **service** {*ma-name* | *ma-number* | *vpn-id*}—Use the same service identifier that was used for configuring CVLAN Service above in Step3.
Step 11	`Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 12	`Switch# show ethernet cfm maintenance-points local`	Verify the configuration.
Step 13	`Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

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

This is a sample configuration for a CVLAN Up MEP:

```
Switch(config)# ethernet cfm domain abc level 3
Switch(config-ecfm)# service CVLANMEP vlan 10 inner-vlan 20
Switch(config-ecfm-srv)# continuity-check
Switch(config-ecfm-srv)# exit
Switch(config-ecfm)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ethernet cfm mep domain abc mpid 1020 service CVLANMEP
Switch(config-if)# end
```

Similarly, a manual configuration of MIP for CVLAN is configured using the **ethernet cfm mip level** *level-id* **vlan** *svlan-id* **inner-vlan** *cvlan-id* command.

Feature Support and Behavior

CFM S-VLAN component support:

- Up MEPs at any level (0 to 7).

  Up MEPs use the port access VLAN ID (the outer tag or S-VLAN).

  CFM frames sent and received by Up MEPs have a single VLAN tag, and the VLAN identifier is the port access VLAN ID (S-VLAN). Because the 802.1q tunnel interface marks the endpoint of the S-VLAN, the associated S-VLAN component should mark the endpoint of the CFM domain running over the S-VLAN space.

CFM C-VLAN component support:

- Up MEP functions at any level (0 to 7).

  Up MEPs use two tags: an outer tag with a VLAN ID that is the port access VLAN (S-VLAN) and an inner tag with a selected C-VLAN that is allowed through the 802.1q tunnel port. CFM frames sent and received by these Up MEPs are always double-tagged.

- MIP functions at any level (0 to 7).

  MIPs process CFM frames that are single-tagged when coming from the wire-side and double-tagged when coming from the relay-function side.

- Transparent point functions.

Supported maintenance points on 802.1q tunnels:

- Up MEP on the C-VLAN component for selective or all-to-one bundling
- Up MEP on the S-VLAN
- Port MEP
- MIP support on C-VLAN component for selective or all-to-one bundling

Note The switch supports only manual configuration of MIPs. It does not support MIP autocreation on C-VLANs.

Platform Restrictions and Limitations

- Maximum supported MEPs per switch at each continuity check message (CCM) interval:
  - 1600 MEP local and 1600 MEP remote (on C-VLAN and S-VLAN) with 10-second intervals
  - 250 MEP local and 250 MEP remote (on C-VLAN and S-VLAN) with 1-second intervals
- Maximum supported MIPs at each CCM interval:
  - 300 MIPs at 10 seconds
  - 125 MIPs at 1 second
- There could be issues detecting cross-connect errors on the Catalyst 4500 Series Switch.
- These features are not supported:
  - CFM C-component on the native VLAN
  - Down MEP on S or C-VLAN (provider network port)
  - MIP on S-VLAN (provider network port)
  - CFM C-VLAN alarm indication signal (AIS)

- 802.3ah interworking with CFM C-VLAN
- CFM C-VLAN IP SLAs
- CFM C-VLAN MIP autocreation
- CFM C-VLAN with One-to-One VLAN mapping on Trunk ports.

Understanding CFM ITU-T Y.1731 Fault Management

The ITU-T Y.1731 feature provides new CFM functionality for fault and performance management for service providers in large network. The switch supports Ethernet Alarm Indication Signal (ETH-AIS), Ethernet Remote Defect Indication (ETH-RDI), Ethernet Locked Signal (ETH-LCK), and Ethernet Multicast Loopback Message (MCAST-LBM) functionality for fault detection, verification, and isolation.

Y.1731 Terminology

- Server MEP—the combination of the server layer termination function and server or Ethernet adaptation layer termination function or server or Ethernet adaptation function, where the server layer termination function is expected to run OAM mechanisms specific to the server layer. The supported mechanisms are link up, link down, and 802.3ah.
- Server layer—a virtual MEP layer capable of detecting fault conditions.
- Defect conditions:
  - Loss of continuity (LOC): the MEP stopped receiving CCM frames from a peer MEP
  - Mismerge: the MEP received a CCM frame with a correct maintenance level (matching the MEP level) but an incorrect maintenance ID.
  - Unexpected MEP: the MEP received a CCM frame with the correct maintenance level (matching the MEP's level) and correct maintenance ID, but an unexpected MEP ID.
  - Unexpected maintenance level: the MEP received a CCM frame with an incorrect maintenance level.
  - Unexpected period: the MEP received a CCM frame with a correct maintenance level, a correct maintenance ID, a correct MEP ID, but a different transmission period field.
- Signal fail—the MEP declares a signal fail condition when it detects a defect condition.
- Alarm Indication Signal (AIS) condition—the MEP received an AIS frame.
- Remote Defect Indication (RDI) condition—The MEP received a CCM frame with the RDI field set.

Alarm Indication Signals

The Ethernet Alarm Signal function (ETH-AIS) is used to suppress alarms after defects are detected at the *server* (sub) layer, which is a virtual MEP layer capable of detecting fault conditions. A fault condition could be a signal fail condition, an AIS condition, or a LCK condition.

Note Although the configuration is allowed, you should not configure AIS in networks running STP. An STP configuration might cause AIS interruption or redirection.

When a MEP or a service MEP (SMEP) detects a connectivity fault at a specific maintenance association level, it multicasts AIS frames in the direction away from the detected failure at the client maintenance association level. The frequency of AIS frame transmission is based on the AIS transmission period. The first AIS frame is always sent immediately following the detection of the defect condition. We recommend a transition period of 1 second in a network of only a few VLANs to ensure that the first AIS frame is sent immediately following error detection. We recommend a 60-second interval in a network of multiple (up to 4094) VLANs to prevent stressing the network with 1-second transmissions.

A MEP that receives a frame with ETH-AIS information cannot determine the specific server with the defect condition or the set of peer MEPs for which it should suppress alarms. Therefore, it suppresses alarms for all peer MEPs, whether or not they are connected.

When a MEP receives an AIS frame, it examines it to be sure that the Maintenance Entity Group (MEG) level matches its own MEG and then detects the AIS default condition. (A MEG is Y.1731 terminology for maintenance association in 802.1ag.) After this detection, if no AIS frames are received for an interval of 3.5 times the AIS transmission period, the MEP clears the AIS defect condition. For example, if the AIS timer is set for 60 seconds, the AIS timer period expires after 3.5 times 60, or 210 seconds.

The AIS condition is terminated when a valid CCM is received with all error conditions cleared or when the AIS period timer expires (the default time is 60 seconds).

Ethernet Remote Defect Indication

When Ethernet OAM continuity check (ETH-CC) transmission is enabled, the Ethernet Remote Defect Indication (ETH-RDI) function uses a bit in the CFM CC message to communicate defect conditions to the MEP peers. For ETH-RDI functionality, you must configure the MEP MEG level, the ETH-CC transmission period, and the ETH-CC frame priority. ETH-RDI does not require any MIP configuration.

When a MEP receives frames with ETH-RDI information, it determines that its peer MEP has encountered a defect condition and sets the RDI files in the CCM frames for the duration of the defect condition. When the defect condition clears, the MEP clears the RDI field.

When a MEP receives a CCM frame, it examines it to ensure that its MEG level is the same and if the RDI field is set, it detects an RDI condition. For point-to-point Ethernet connections, a MEP can clear the RDI condition when it receives the first frame from its peer MEP with the RDI field cleared. However, for multipoint Ethernet connectivity, the MEP cannot determine the associated subset of peer MEPs with which the sending MEP has seen the defect condition. It can clear the RDI condition after it receives CCM frames with the RDI field cleared from its entire list of peer MEPs.

Multicast Ethernet Loopback

The multicast Ethernet loopback (ETH-LB) function verifies bidirectional connectivity of a MEP with its peer MEPs and is an on-demand OAM function. When the feature is invoked on a MEP by entering the **ping** privileged EXEC command, the MEP sends a multicast frame with ETH-LB request information to peer MEPs in the same MEG. The MEP expects to receive a unicast frame with ETH-LB reply information from its peer MEPs within a specified time period. A MEP receiving a multicast frame with ETH-LB request information validates the frame and transmits a frame with reply information.

To configure multicast ETH-LB, you configure the MEG level of the MEP and the priority of the multicast frames with ETH-LB requests. Multicast frames with ETH-LB request information are always marked as drop ineligible. No MIP configuration is required.

The MEP sends multicast LB message frames on an on-demand basis. After sending a multicast LBM frame, the MEP expects to receive LB reply frames within 5 seconds.

When a MEP receives a valid LBM frame, it generates an LB reply frame and sends it to the requested MEP after a random delay in the range of 0 to 1 second. The validity of the frame is determined on its having the correct MEG level.

When a MEP sends a multicast LBM frame and receives an LB reply frame within 5 seconds, the LB reply frame is valid.

Configuring Y.1731 Fault Management

To configure Y.1731 fault management, you must enable CFM and configure MIPs on the participating interfaces. AIS messages are generated only on interfaces with a configured MIP.

Default Y.1731 Configuration

ETH-AIS and ETH-LCK are enabled by default when CFM is enabled.

When you configure ETH-AIS or ETH-LCK, you must configure CFM before ETH-AIS or ETH-LCK is operational.

ETH-RDI is set automatically when continuity check messages are enabled.

Configuring ETH-AIS

Beginning in privileged EXEC mode, follow these steps to configure Ethernet AIS on a switch:

	Command	Purpose
Step 1	`configure terminal`	Enters global configuration mode.
Step 2	`ethernet cfm ais link-status global`	Configures AIS-specific SMEP commands by entering config-ais-link-cfm mode.

	Command	Purpose
Step 3	**level** *level-id* or disable	Configures the maintenance level for sending AIS frames transmitted by the SMEP. The range is 0 to 7. or Disables generation of ETH-AIS frames.
Step 4	**period** *value*	Configures the SMEP AIS transmission period interval. Allowable values are 1 second or 60 seconds.
Step 5	**exit**	Returns to global configuration mode.
Step 6	**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 7	**service** {*ma-name* | *ma-number* | *vpn-id vpn*} {**vlan** *vlan-id* [**direction down**] | **port**}	Defines a customer service maintenance association (MA) name or number to be associated with the domain, or a VLAN ID or VPN-ID, and enter ethernet-cfm-service configuration mode. • *ma-name*—a string of no more than 100 characters that identifies the MAID. • *ma-number*—a value from 0 to 65535. • *vpn-id*—enter a VPN ID as the *ma-name*. • **vlan** *vlan-id*—VLAN range is from 1 to 4094. You cannot use the same VLAN ID for more than one domain at the same level. • (Optional) **direction down**—specify the service direction as down. • **port**—Configure port MEP, a down MEP that is untagged and not associated with a VLAN.
Step 8	**ais level** *level-id*	(Optional) Configures the maintenance level for sending AIS frames transmitted by the MEP. The range is 0 to 7.
Step 9	**ais period** *value*	(Optional) Configures the MEP AIS transmission period interval. Allowable values are 1 second or 60 seconds.
Step 10	**ais expiry-threshold** *value*	(Optional) Sets the expiring threshold for the MA as an integer. The range is 2 to 255. The default is 3.5.
Step 11	**no ais suppress-alarms**	(Optional) Overrides the suppression of redundant alarms when the MEP goes into an AIS defect condition after receiving an AIS message.
Step 12	**exit**	Returns to ethernet-cfm configuration mode.
Step 13	**exit**	Returns to global configuration mode.
Step 14	**interface** *interface-id*	Specifies an interface ID, and enter interface configuration mode.
Step 15	[**no**] **ethernet cfm ais link-status**	Enables or disable sending AIS frames from the SMEP on the interface.
Step 16	**ethernet cfm ais link-status period** *value*	Configures the ETH-AIS transmission period generated by the SMEP on the interface. Allowable values are 1 second or 60 seconds.

	Command	Purpose
Step 17	**ethernet cfm ais link-status level** *level-id*	Configures the maintenance level for sending AIS frames transmitted by the SMEP on the interface. The range is 0 to 7.
Step 18	**end**	Returns to privileged EXEC mode.
Step 19	**show ethernet cfm smep** [**interface** *interface-id*]	Verifies the configuration.
Step 20	**show ethernet cfm error**	Displays received ETH-AIS frames and other errors.
Step 21	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

Use the **no** form of the commands to return to the default configuration or to remove a configuration. To disable the generation of ETH-AIS frames, enter the **disable** config-ais-link-cfm mode command.

This is an example of the output from the **show ethernet cfm smep** command when Ethernet AIS has been enabled:

```
Switch# show ethernet cfm smep
SMEP Settings:
--------------
Interface: GigabitEthernet1/0/3
LCK-Status: Enabled
LCK Period: 60000 (ms)
Level to transmit LCK: Default
AIS-Status: Enabled
AIS Period: 60000 (ms)
Level to transmit AIS: Default
Defect Condition: AIS
```

Using Multicast Ethernet Loopback

You can use the **ping** privileged EXEC command to verify bidirectional connectivity of a MEP, as in this example:

```
Switch# ping ethernet multicast domain CD vlan 10
Type escape sequence to abort.
Sending 5 Ethernet CFM loopback messages to 0180.c200.0037, timeout is 5 seconds:
Reply to Multicast request via interface FastEthernet1/0/3, from 001a.a17e.f880, 8 ms
Total Loopback Responses received: 1
```

Managing and Displaying Ethernet CFM Information

You can use the privileged EXEC commands in these tables to clear Ethernet CFM information.

Table 1 Clearing CFM Information

Command	Purpose
clear ethernet cfm ais domain *domain-name* **mpid** *id* {**vlan** *vlan-id* | **port**}	Clears MEPs with matching domain and VLAN ID out of AIS defect condition.
clear ethernet cfm ais link-status interface *interface-id*	Clears a SMEP out of AIS defect condition.
clear ethernet cfm error	Clears all CFM error conditions, including AIS.

You can use the privileged EXEC commands in Table 46-2 to display Ethernet CFM information.

Table 46-2 Displaying CFM Information

Command	Purpose
show ethernet cfm domain [brief]	Displays CFM domain information or brief domain information.
show ethernet cfm errors [configuration | domain-id]	Displays CFM continuity check error conditions logged on a device since it was last reset or the log was last cleared. When CFM crosscheck is enabled, displays the results of the CFM crosscheck operation.
show ethernet cfm maintenance-points local [detail | domain | interface | level | mep | mip]	Displays maintenance points configured on a device.
show ethernet cfm maintenance-points remote [crosscheck | detail | domain | static]	Displays information about a remote maintenance point domains or levels or details in the CFM database.
show ethernet cfm mpdb	Displays information about entries in the MIP continuity-check database.
show ethernet cfm smep [**interface** *interface-id*]	Displays Ethernet CFM SMEP information.
show ethernet cfm traceroute-cache	Displays the contents of the traceroute cache.

This is an example of output from the **show ethernet cfm domain brief** command:

```
Switch# show ethernet cfm domain brief
Domain Name                                Index Level Services Archive(min)
level5                                         1     5        1     100
level3                                         2     3        1     100
test                                           3     3        3     100
name                                           4     3        1     100
test1                                          5     2        1     100
lck                                            6     1        1     100Total Services : 1
```

This is an example of output from the **show ethernet cfm errors** command:

```
Switch# show ethernet cfm errors
-------------------------------------------------------------------------------
MPID Domain Id                                 Mac Address     Type   Id  Lvl
     MAName                                    Reason                 Age
-------------------------------------------------------------------------------
6307 level3                                    0021.d7ee.fe80  Vlan   7    3
     vlan7                                     Receive RDI            5s
```

This is an example of output from the **show ethernet cfm maintenance-points local detail** command:

```
Switch# show ethernet cfm maintenance-points local detail
Local MEPs:
----------
MPID: 7307
DomainName: level3
Level: 3
Direction: Up
Vlan: 7
Interface: Gi0/3
CC-Status: Enabled
CC Loss Threshold: 3
MAC: 0021.d7ef.0700
LCK-Status: Enabled
LCK Period: 60000(ms)
LCK Expiry Threshold: 3.5
```

```
Level to transmit LCK: Default
Defect Condition: No Defect
presentRDI: FALSE
AIS-Status: Enabled
AIS Period: 60000(ms)
AIS Expiry Threshold: 3.5
Level to transmit AIS: Default
Suppress Alarm configuration: Enabled
Suppressing Alarms: No


MIP Settings:
-------------
Local MIPs:
* = MIP Manually Configured
------------------------------------------------------------------------------
 Level Port           MacAddress     SrvcInst   Type    Id
------------------------------------------------------------------------------
*5     Gi0/3          0021.d7ef.0700 N/A        Vlan    2,7
```

This is an example of output from the **show ethernet cfm traceroute** command:

```
Switch# show ethernet cfm traceroute
Current Cache-size: 0 Hops
Max Cache-size: 100 Hops
Hold-time: 100 Minutes
```

You can use the privileged EXEC commands in Table 46-3 to display IP SLAs Ethernet CFM information.

Table 46-3 Displaying IP SLAs CFM Information

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