



# ethernet cfm mep crosscheck through location prefer

---

- [ethernet cfm mep crosscheck, on page 3](#)
- [ethernet cfm mep crosscheck start-delay, on page 6](#)
- [ethernet cfm mep domain mpid, on page 7](#)
- [ethernet cfm mep level mpid vlan, on page 9](#)
- [ethernet cfm mip, on page 12](#)
- [ethernet cfm mip level, on page 14](#)
- [ethernet cfm slm max, on page 16](#)
- [ethernet cfm slm timeout, on page 17](#)
- [ethernet cfm traceroute cache, on page 18](#)
- [ethernet cfm traceroute cache hold-time, on page 19](#)
- [ethernet cfm traceroute cache size, on page 21](#)
- [ethernet event microwave, on page 23](#)
- [ethernet evc, on page 25](#)
- [ethernet lmi, on page 27](#)
- [ethernet lmi ce-vlan map, on page 29](#)
- [ethernet lmi global, on page 31](#)
- [ethernet lmi interface, on page 32](#)
- [ethernet loopback local interface, on page 33](#)
- [ethernet loopback permit, on page 34](#)
- [ethernet mac-flush notification mirp, on page 36](#)
- [ethernet mac limit action flooding disable, on page 37](#)
- [ethernet mac limit maximum addresses, on page 39](#)
- [ethernet mac-tunnel virtual, on page 40](#)
- [ethernet oam, on page 41](#)
- [ethernet oam link-monitor frame, on page 44](#)
- [ethernet oam link-monitor frame-period, on page 46](#)
- [ethernet oam link-monitor frame-seconds, on page 48](#)
- [ethernet oam link-monitor high-threshold action, on page 50](#)
- [ethernet oam link-monitor on, on page 52](#)
- [ethernet oam link-monitor receive-crc, on page 53](#)
- [ethernet oam link-monitor supported, on page 55](#)

- ethernet oam link-monitor symbol-period, on page 57
- ethernet oam link-monitor transmit-crc, on page 59
- ethernet oam mib log size, on page 61
- ethernet oam remote-failure, on page 62
- ethernet oam remote-loopback, on page 64
- ethernet oam remote-loopback (interface), on page 66
- ethernet ring g8032, on page 68
- ethernet ring g8032 profile, on page 69
- ethernet subscriber, on page 70
- ethernet subscriber session, on page 71
- ethernet subscriber static, on page 73
- ethernet tcn-propagation, on page 75
- ethernet uni, on page 76
- event ethernet microwave clear-sd, on page 78
- event ethernet microwave sd, on page 79
- exclusion-list, on page 81
- id (CFM), on page 82
- inclusion-list, on page 83
- ingress-replication, on page 84
- initiator unclassified vlan, on page 85
- input, on page 86
- l2 subscriber, on page 87
- lacp active-port distribution automatic, on page 89
- lacp direct-loadswap, on page 91
- lacp failover, on page 92
- lacp fast-switchover, on page 94
- lacp max-bundle, on page 96
- lacp min-bundle, on page 98
- lacp port-priority, on page 100
- lacp rate, on page 102
- lacp system-priority, on page 103
- level (CFM-AIS-link), on page 105
- level, on page 106
- lldp, on page 107
- lldp enable, on page 109
- lldp (interface), on page 110
- location, on page 111
- location (interface), on page 112
- location civic-location identifier, on page 114
- location civic-location-id, on page 117
- location custom-location identifier, on page 120
- location custom-location-id, on page 122
- location geo-location identifier, on page 124
- location geo-location-id, on page 126
- location prefer, on page 128
- show-macsec-post, on page 129

# ethernet cfm mep crosscheck

To enable cross-checking between the list of configured remote maintenance endpoints (MEPs) of a domain and MEPs learned through continuity check messages (CCMs), use the **ethernet cfm mep crosscheck** command in privileged EXEC mode or global configuration mode. To disable cross-checking, use the **ethernet cfm mep crosscheck disable** command.

## Cisco Prestandard Connectivity Fault Management Draft 1 (CFM D1)

```
ethernet cfm mep crosscheck {enable | disable} level {level-id | level-id-level-id [,level-id-level-id]}
{vlan {vlan-id | any | vlan-id-vlan-id [,vlan-id-vlan-id]} | evc evc-name}
```

## CFM IEEE 802.1ag Standard (CFM IEEE)

```
ethernet cfm mep crosscheck {enable | disable} domain domain-name {port | vlan {vlan-id |
vlan-id-vlan-id | ,vlan-id-vlan-id}}
```

## Cisco IOS XE Release 3.7S for Cisco Series ASR 1000 Routers

```
ethernet cfm mep crosscheck {enable | disable} domain domain-name service {short-ma-name | icc
icc-code meg-id | number ma-number | vlan-id vlan-id | vpn-id vpn-id}
```

Syntax Description		
<b>enable</b>		Indicates that cross-checking will occur.
<b>disable</b>		Indicates that cross-checking will not occur.
<b>level</b> <i>level-id</i>		Indicates a maintenance level for configuration. Integer from 0 to 7 that identifies the maintenance level.
<i>, level-id - level-id</i>		(Optional) Integer values from 0 to 7. The comma must be entered to separate level ID ranges. The hyphen is required to separate starting and ending level ID values that are used to define each range of IDs.
<b>vlan</b> <i>vlan-id</i>		Indicates a VLAN for cross-checking. Integer from 1 to 4094 that identifies the VLAN.
<i>level-id - level-id</i>		Integer values from 0 to 7. The hyphen is required to separate starting and ending level ID values that are used to define the range of IDs.
<b>any</b>		Indicates that all VLANs are to be configured. <ul style="list-style-type: none"> <li>This option is supported only in CFM D1.</li> </ul>
<b>evc</b> <i>evc-name</i>		String that associates an Ethernet virtual connection (EVC) to the service instance. Maximum: 100 bytes.
<b>domain</b> <i>domain-name</i>		Specifies the domain where the destination MEP resides. Maximum: 154 characters.
<b>service</b>		Specifies the maintenance association (MA) within the domain.

<i>short-ma-name</i>	The short-name identifier for the MA service. The domain name and short MA name combined cannot exceed 48 bytes.
<b>icc</b> <i>icc-code meg-id</i>	ITU Carrier Code (ICC) (maximum: 6 characters) and unique maintenance entity group (MEG) ID Code (UMC) (maximum: 12 characters).
<b>number</b> <i>ma-number</i>	The MA number. Range: 0 to 65535.
<b>vlan-id</b> <i>vlan-id</i>	The primary VLAN ID. Range: 1 to 4094.
<b>vpn-id</b> <i>vpn-id</i>	The VPN ID. Range: 1 to 32767.

**Command Modes**

Privileged EXEC (#)

Global configuration (config)

**Command History**

<b>Release</b>	<b>Modification</b>
12.2(33)SRA	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRD	The <b>evc</b> keyword and <i>evc-name</i> argument were added on the Cisco 7600 Series Route Switch Processor 720 (RSP 720) and the Cisco 7600 Series Supervisor Engine 720.
12.2(33)SXI2	This command was integrated into Cisco IOS Release 12.2(33)SXI2.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
Cisco IOS XE Release 3.7S	This command was modified. The <b>port</b> , <b>vlan</b> , and <b>evc</b> keywords were deprecated and options to specify the MA service via the <b>service</b> keyword were introduced.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.

**Usage Guidelines**

Before you issue this command, you must configure a static list of MEPs using the **mep crosscheck mpid vlan** command. To enable cross-checking after a device has booted up, you must issue the **ethernet cfm mep crosscheck enable** command.

A **no** form of this command does not exist. Cross-checking is disabled when you issue the command with the **disable** keyword.

In CFM IEEE, if a domain name has more than 43 characters, a warning message is displayed notifying that the maintenance domain ID (MDID) will be truncated to 43 characters in continuity check messages if “id <fmt> <MDID>” is not configured.

To view the results of a cross-check operation, use the **show ethernet cfm maintenance-points remote crosscheck** command. To view errors in the cross-check operation, use the **show ethernet cfm errors** command. Both commands are used in privileged EXEC mode.

Traps are generated after a cross-check operation is completed if cross-check traps are already enabled and, if as the result of the cross-check operation, a condition warrants a trap to be sent.

## Examples

The following example shows how to enable an Ethernet CFM MEP cross-check on an MEP in CFM IEEE:

```
Device# ethernet cfm mep crosscheck enable domain customerA service zzz
```

The following example shows how to enable an Ethernet CFM MEP cross-check in CFM D1 at level 2 for VLAN IDs in the range from 3000 to 3375:

```
Device# ethernet cfm mep crosscheck enable level 2 vlan 3000-3375
```

## Related Commands

Command	Description
<b>mep crosscheck mpid vlan</b>	Statically defines a remote MEP within a maintenance domain.
<b>show ethernet cfm errors</b>	Displays CFM continuity check error conditions logged on a device since it was last reset or since the log was last cleared.
<b>show ethernet cfm maintenance-points remote crosscheck</b>	Displays detailed information about remote MEPs in the cross-check list that were statically configured.

# ethernet cfm mep crosscheck start-delay

To configure the maximum amount of time that a device waits for remote maintenance endpoints (MEPs) to come up before the cross-check operation is started, use the **ethernet cfm mep crosscheck start-delay** command in global configuration mode. To restore the default number of seconds a device waits, use the **no** form of this command.

**ethernet cfm mep crosscheck start-delay** *delay*  
**no ethernet cfm mep crosscheck start-delay** *delay*

## Syntax Description

<i>delay</i>	Integer from 1 to 65535 that specifies the number of seconds a device waits for remote MEPs to come up before the cross-check is started. The default is 30.
--------------	--

## Command Default

The start delay interval is enabled with a default of 30 seconds.

## Command Modes

Global configuration (config)

## Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SXI2	This command was integrated into Cisco IOS Release 12.2(33)SXI2.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.

## Usage Guidelines

If continuity check intervals in your network are greater than 30 seconds (the delay default), you must configure the start-delay to match the greatest interval to avoid unnecessary traps.

When the default value is configured, “ethernet cfm mep crosscheck start-delay 30” is displayed when the **show running all** command is issued.

## Examples

The following example shows how to set the maximum number of seconds that a device will wait for remote MEPs to come up before the cross-check operation is started to 700:

```
Device(config)# ethernet cfm mep crosscheck start-delay 700
```

## Related Commands

Command	Description
<b>show running all</b>	Shows the running configuration with default values.

# ethernet cfm mep domain mpid

To set a port as internal to a maintenance domain and define it as a maintenance endpoint (MEP), use the **ethernet cfm mep domain mpid** command in interface configuration mode. To restore the default configuration of the port, use the **no** form of this command.

```
ethernet cfm mep domain domain-name mpid mpid {port | vlan vlan-id}
no ethernet cfm mep domain domain-name mpid mpid {port | vlan vlan-id}
```

## Cisco IOS XE Release 3.7S for Cisco Series ASR 1000 Router

```
ethernet cfm mep domain domain-name mpid mpid service {short-ma-name | icc icc-code meg-id
| number ma-number | vlan-id vlan-id | vpn-id vpn-id}
no ethernet cfm mep domain domain-name mpid mpid service {short-ma-name | icc icc-code meg-id
| number ma-number | vlan-id vlan-id | vpn-id vpn-id}
```

### Syntax Description

<i>domain-name</i>	String. Maximum: 154 characters.
<i>mpid</i>	Integer that identifies the MEP. Range: 1 to 8191.
<b>port</b>	Specifies a DOWN service direction with no VLAN associations (untagged).
<b>vlan</b> <i>vlan-id</i>	Indicates a VLAN for cross-checking. Integer from 1 to 4094 that identifies the VLAN.
<b>service</b>	Specifies the maintenance association (MA) within the domain.
<i>short-ma-name</i>	The short-name identifier for the MA service. The domain name and short MA name combined cannot exceed 48 bytes.
<b>icc</b> <i>icc-code meg-id</i>	ITU Carrier Code (ICC) (maximum: 6 characters) and unique maintenance entity group (MEG) ID Code (UMC) (maximum: 12 characters).
<b>number</b> <i>ma-number</i>	The MA number. Range: 0 to 65535.
<b>vlan-id</b> <i>vlan-id</i>	The primary VLAN ID. Range: 1 to 4094.
<b>vpn-id</b> <i>vpn-id</i>	The VPN ID. Range: 1 to 32767.

### Command Default

This default port-maintenance configuration applies.

### Command Modes

Interface configuration (config-if)

### Command History

Release	Modification
12.2(33)SXI2	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Release	Modification
Cisco IOS XE 3.7S	This command was modified.  The <b>port</b> and <b>vlan</b> keywords were deprecated and options to specify the MA service via the <b>service</b> keyword were introduced.
Cisco IOS 15.4(3)S	This command was implemented on Cisco ME 2600X Series Ethernet Access Switches.

### Usage Guidelines

You can use this command to place the CLI in Ethernet connectivity fault management (CFM) MEP configuration mode (config-if-ecfm-mep).

A single interface may belong to multiple domains, meaning that you can issue multiple instances of the **ethernet cfm mep domain mpid** command for different domains.

If a specified domain has not been configured, an error message is displayed and the command is rejected.

If an interface is manually provisioned to have a maintenance intermediate point (MIP) at a certain maintenance level and you attempt to configure it as a MEP for a VLAN on the same or a higher level, an error message is displayed and the command is rejected.

If the VLAN for which a MEP is configured is removed from an interface, the MEP configuration is also removed; the VLAN and the definition of the MEP are interrelated.

If a domain name is longer than 43 characters, a warning message is displayed notifying that the maintenance domain ID (MDID) will be truncated to 43 characters in continuity check messages (CCMs) if “id <fmt> <MDID>” is not configured.

In Cisco IOS XE Release 3.7S and later releases, configuring the **ethernet cfm mep domain mpid** command using the **port** and **vlan** keywords is rejected when there are multiple MAs mapping to the same service in the domain.

### Examples

The following example shows how to set a service as internal to a maintenance domain, define it as a maintenance endpoint (MEP), and configure the service zzz:

```
Device(config)# interface ethernet 0/1
Device(config-if)# ethernet cfm mep domain CustomerB mpid 5 service zzz
Device(config-if)#
```



## ethernet cfm mep level mpid vlan

To set an interface as a domain boundary (edge), define it as a maintenance endpoint (MEP), and set the direction for the MEP, use the **ethernet cfm mep level mpid vlan** command in interface configuration mode. To restore the default configuration of the interface, use the **no** form of this command.

```
ethernet cfm mep level level-id [{inward | outward domain domain-name}] mpid id vlan
{anyvlan-id,vlan-id | vlan-id-vlan-id | ,vlan-id-vlan-id}
no ethernet cfm mep level level-id [{inward | outward domain domain-name}] mpid id vlan
{anyvlan-id,vlan-id | vlan-id-vlan-id | ,vlan-id-vlan-id}
```

### Syntax Description

<i>level-id</i>	Integer from 0 to 7 that identifies the maintenance level at which the MEP is defined.
<b>inward</b>	(Optional) Indicates the direction of the MEP is toward the device. This is the default.
<b>outward</b>	(Optional) Sets an interface as outward (toward the wire).
<b>domain</b>	(Optional) Identifies the domain in which the MEP will be configured.
<i>domain-name</i>	(Optional) String of a maximum of 154 characters that identifies the domain.
<i>id</i>	Integer from 0 to 8191 that identifies the MEP.
<b>any</b>	Indicates all VLANs are to be configured.
<i>vlan-id</i>	Integer from 1 to 4094 that identifies a VLAN to be configured.
<i>, vlan-id</i>	Integers from 1 to 4094, separated by commas, that list VLANs to be configured.
<i>vlan-id - vlan-id</i>	Integers from 1 to 4094 that define a range of VLANs to be configured. The hyphen is required to separate starting and ending values that are used to define the range.
<i>, vlan-id - vlan-id</i>	Integers from 1 to 4094 that define a list of VLAN ranges to be configured. The comma must be entered to separate ranges. The hyphen is required to separate starting and ending values that are used to define each range of VLANs.

### Command Default

No MEPs are configured until this command is issued.

### Command Modes

Interface configuration (config-if)

### Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T. The <b>outward</b> and <b>domain</b> keywords and the <i>domain-name</i> argument were added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Release	Modification
12.2(33)SRD	This command was modified. Support was added for outward facing MEPs on switch ports on Cisco 7600 series routers.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.

## Usage Guidelines

Following is the order in which you must configure Ethernet connectivity fault management (CFM) elements:

1. Domain at the same level as the MEP to be configured
2. Service within the domain
3. Maintenance intermediate point (MIP) at a level higher than the MEP if the domain is not an outward domain
4. MEP

If you do not configure elements in this sequence, the **ethernet cfm mep level mpid vlan** command will fail. An exception is at maintenance level 7, where configuring a MIP on the interface before you configure a MEP is not required. Configuring a MIP on an interface also is not required when you are configuring an outward facing MEP.

A single interface may belong to multiple domains, which means you can issue multiple instances of the **ethernet cfm mep level mpid vlan** command for different domains and for different VLANs.

More than one domain can be configured at a single level. The level plus VLAN indicates the domain to which the MEP belongs.

You can configure a single MEP, a list of MEPs, or a range of MEPs so that there is one MEP per VLAN and all MEPs share the same level, direction, and maintenance endpoint ID (MPID).

If the direction of the MEP is not stated, the default is inward facing (toward the Bridge). When you specify an outward MEP, you must provide a domain name. If the specified domain has not been configured or if the specified domain has not been tagged as outward, an error message will display and the command will be rejected.

All MEPs and MIPs must be removed from an interface before MEPs at level 7 can be configured. Also, when you remove MEP configurations at Level 7, you should first remove all lower level MEPs. If you try to configure a MEP on an interface with a level higher than the MIP level, the command will be rejected and an error message will be displayed.

If an interface is provisioned to be a MIP for a certain maintenance level and you try to configure the interface as an inward MEP for a VLAN at the same level, the command will be rejected and an error message will display. If a VLAN for which a MEP is configured is removed from an interface, the MEP configuration remains, but the MEP is inactive and does not transmit or receive messages because the definition of the MEP is associated with the VLAN.

## Examples

The following example shows how to set interface Ethernet 0/1 as a domain boundary and define it as a MEP at level 5, with a MPID of 5 on VLAN 101, and then issue the **show ethernet cfm maintenance-points local** command to display the list of configured MEPs in the device:

```
Device(config)# interface ethernet 0/1
```

```
Device(config-if)# ethernet cfm mep level 5 mpid 5 vlan 101
Device(config-if)# Ctrl-Z
Device(config)# show ethernet cfm maintenance-points local
```

The following example shows how to set interface Ethernet 0/1 as outward for maintenance domain domain1 and define it as a MEP at level 5 with the MEP ID 700 on VLAN 5:

```
Device(config)# interface ethernet 0/1
Device(config-if)# ethernet cfm mep level 5 outward domain domain1 mpid 700 vlan 5
```

The following example shows how to set interface Ethernet 5/0 as a domain boundary and define it as a MEP at level 7, with a MPID of 3001 on VLAN 100 on a switch port:

```
Device(config)# interface ethernet 5/0
Device(config-if)# switchport
Device(config-if)# switchport mode trunk
Device(config-if)# ethernet cfm mep level 7 outward domain CUSTOMER mpid 3001 vlan 100
```

The following example shows how to set interface Ethernet 5/0 as a domain boundary and define it as a MEP at level 7, with a MPID of 3001 on VLAN 100 on a routed port:

```
Device(config)# interface ethernet 5/0
Device(config-if)# ethernet cfm mep level 7 outward domain CUSTOMER mpid 3001 vlan 100
!
Device(config-if)# interface Ethernet5/0.100
Device(config-if)# encapsulation dot1Q 100
```

#### Related Commands

Command	Description
<b>ethernet cfm domain</b>	Defines a CFM domain at a specified maintenance level.
<b>ethernet cfm mip level</b>	Provisions a MIP at a specified maintenance level on an interface.
<b>service vlan</b>	Sets a universally unique ID for a customer service instance within a maintenance domain.
<b>show ethernet cfm maintenance-points local</b>	Displays maintenance points configured on a device.

# ethernet cfm mip

To globally provision maintenance intermediate points (MIPs) at a specified maintenance level for VLAN IDs that are not associated with specific maintenance associations (MAs) and to enable level filtering, use the **ethernet cfm mip** command in global configuration mode. To remove a MIP, use the **no** form of this command.

```
ethernet cfm mip {auto-create level level-id vlan {vlan-id | vlan-id-vlan-id | ,vlan-id-vlan-id}
[lower-mep-only] [sender-id chassis] | filter}
no ethernet cfm mip {auto-create level level-id vlan {vlan-id | vlan-id-vlan-id | ,vlan-id-vlan-id}
[lower-mep-only] [sender-id chassis] | filter}
```

## Syntax Description

<b>auto-create</b>	Dynamically creates a connectivity fault management (CFM) MIP.
<b>level</b>	Specifies a maintenance domain level.
<i>level-id</i>	Integer from 0 to 7 that identifies the maintenance level.
<b>vlan</b>	Indicates a VLAN for configuration.
<i>vlan-id</i>	Integer from 1 to 4094 that identifies the VLAN to be configured.
<i>vlan-id -vlan-id</i>	Integers from 1 to 4094 that define a range of VLANs to be configured. <ul style="list-style-type: none"> <li>The hyphen is required to separate the starting and ending VLAN ID values that are used to define the range of VLAN IDs.</li> </ul>
<i>,vlan-id-vlan-id</i>	Integers from 1 to 4094 that define a range of VLANs to be configured. <ul style="list-style-type: none"> <li>The comma is required to separate VLAN ranges.</li> </ul>
<b>lower-mep-only</b>	(Optional) Creates a MIP only if a MEP is configured at the next lower active maintenance domain level for the VLAN ID on the port.
<b>sender-id</b>	(Optional) Configures the Sender ID option to send for VLAN IDs that are not associated with specific maintenance associations.  If the <b>sender-id</b> option is not configured, the Sender ID TLV is not included in messages.
<b>chassis</b>	(Optional) Sends the chassis ID.
<b>filter</b>	Configures a CFM MIP filter that drops all CFM frames at a lower level independent of whether they come from the wire or relay function side. <ul style="list-style-type: none"> <li>Level filtering is disabled by default.</li> </ul>

## Command Default

MIPs are not provisioned.

## Command Modes

Global configuration (config)

Command History	Release	Modification
	12.2(33)SXI2	This command was introduced.
	12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
	15.1(2)S	This command was integrated into Cisco IOS Release 15.1(2)S.
	Cisco IOS 15.4(3)S	This command was implemented on Cisco ME 2600X Series Ethernet Access Switches.

### Usage Guidelines

MIPs will be provisioned only if all the policies have been met.

This command has lower precedence than the manual MIP **ethernet cfm mip level** (interface configuration mode) configuration command. For example, if you manually configure a MIP for a particular MA, that configuration overrides the MIP created by the global **ethernet cfm mip** command for that MA.

### Examples

The following example shows how to dynamically create a MIP at maintenance level 6 and configure VLAN 500 if a MEP is configured at the next lower active maintenance domain level for the VLAN ID on the port:

```
Device(config)# ethernet cfm mip auto-create level 6 vlan 500 lower-mep-only
```

### Related Commands

Command	Description
<b>cfm mip level</b>	Sets a port as internal to a maintenance domain, and defines it as a MIP for a MA.
<b>ethernet cfm mip level</b>	Sets a port as internal to a maintenance domain, and defines it as a MIP.

# ethernet cfm mip level

To provision a maintenance intermediate point (MIP) at a specified maintenance level on an interface, use the **ethernet cfm mip level** command in interface configuration mode. To restore the default configuration of the interface, use the **no** form of this command.

## Cisco Pre-Standard Connectivity Fault Management Draft 1 (CFM D1)

```
ethernet cfm mip level level-id
no ethernet cfm mip level level-id
```

## CFM IEEE 802.1ag Standard (CFM IEEE)

```
ethernet cfm mip level level-id [vlan {vlan-id | vlan-id-vlan-id | ,vlan-id-vlan-id}]
no ethernet cfm mip level level-id [vlan {vlan-id | vlan-id-vlan-id | ,vlan-id-vlan-id}]
```

### Syntax Description

<i>level-id</i>	Integer from 0 to 7 that specifies the maintenance levels at which MIPs can be defined.
<b>vlan</b>	(Optional) Indicates a VLAN for configuration.
<i>vlan-id</i>	(Optional) Integer from 1 to 4094 that identifies the VLAN to be configured.
<i>vlan-id - vlan-id</i>	(Optional) Integers from 1 to 4094 that define a valid range of VLANs to be configured. <ul style="list-style-type: none"> <li>The hyphen is required to separate the starting and ending VLAN ID values that are used to define the range of VLAN IDs.</li> </ul>
<i>, vlan-id -vlan-id</i>	(Optional) Integers from 1 to 4094 that define a valid range of VLANs to be configured. <ul style="list-style-type: none"> <li>The comma is required to separate VLAN ranges.</li> </ul>

### Command Default

No MIPs are configured.

### Command Modes

Interface configuration (config-if)

### Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SXI2	This command was integrated into Cisco IOS Release 12.2(33)SXI2.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.

Release	Modification
Cisco IOS 15.4(3)S	This command was implemented on Cisco ME 2600X Series Ethernet Access Switches.

### Usage Guidelines

If you do not configure a VLAN, this command creates MIPs for all VLANs on an interface.

In the CFM D1 implementation, you must first configure a domain using the **ethernet cfm domain** command at the level you want to configure the MIP; otherwise, the **ethernet cfm mip level** command is rejected. In the CFM IEEE implementation, preconfiguring a domain is not required.

You cannot configure a MIP at a level lower than the level of already configured maintenance endpoints (MEPs) on an interface.

Configuring a MIP using this command is known as a manual MIP and has precedence over the **mip auto-create** command.

### Examples

The following example shows how to provision a MIP at maintenance level 5 and then issue the **show ethernet cfm maintenance-points local** command to display the list of configured MIPs in the device:

```
Device(config-if)# ethernet cfm mip level 5
Device(config-if)# Ctrl-Z
Device# show ethernet cfm maintenance-points local
```

### Related Commands

Command	Description
<b>ethernet cfm domain</b>	Defines a CFM domain.
<b>mip auto-create</b>	Enables the automatic creation of a MIP at a maintenance domain level.
<b>show ethernet cfm maintenance-points local</b>	Displays information about maintenance points configured on a device.

# ethernet cfm slm max

To set the maximum number of sessions during which synthetic loss measurement (SLM) frames are transmitted to a maintenance end point (MEP), use the **ethernet cfm slm max** command in global configuration mode. To delete the maximum number of sessions, use the **no** form of this command.

**ethernet cfm slm max** *number-of-sessions*

**no ethernet cfm slm max**

## Syntax Description

<i>number-of-sessions</i>	Number of sessions during which SLM frames are transmitted to a MEP. The default is 8000.  The default for the Cisco 7600 series router is based on the specific line card in use on the router.
---------------------------	--

## Command Default

The maximum number of sessions is not set.

## Command Modes

Global configuration (config)

## Command History

Release	Modification
15.3(1)S	This command was introduced.

## Usage Guidelines

When SLM packets are transmitted, the SLM packets are sent from a device that initiates the transmission. The receiving device then responds accordingly. The **ethernet cfm slm max** command is intended for use at the “responder device” of the transmission path and not at the device initiating the transmission.

After enabling this command, use the **ethernet cfm slm timeout** command to set the amount of time to wait between sessions.

## Examples

The following example shows how to set the maximum number of sessions during which SLM frames are sent to the MEP. In this example, the maximum is set to 1000.

```
Device> enable
Device# configure terminal
Device(config)# ethernet cfm slm max 1000
```

## Related Commands

Command	Description
<b>ethernet cfm slm timeout</b>	Sets the amount of time to wait between sessions during which SLM frames are transmitted to a MEP.



## ethernet cfm slm timeout

To set the amount of time to wait between sessions during which synthetic loss measurement (SLM) frames are transmitted to a maintenance end point (MEP), use the **ethernet cfm slm timeout** command in global configuration mode. To delete the amount of time to wait, use the **no** form of this command.

**ethernet cfm slm timeout** *minutes*

**no ethernet cfm slm timeout**

### Syntax Description

<i>minutes</i>	Time to wait (in minutes) between sessions during which SLM frames are transmitted. Range is 5 and 2400. Default is 5.
----------------	--

### Command Default

The amount of time to wait between sessions is not set.

### Command Modes

Global configuration (config)

### Command History

Release	Modification
15.3(1)S	This command was introduced.

### Usage Guidelines

When SLM packets are transmitted, the SLM packets are sent from a device that initiates the transmission. The receiving device then responds accordingly. The **ethernet cfm slm timeout** command is intended for use at the “responder device” of the transmission path and not at the device initiating the transmission.

Before enabling this command, use the **ethernet cfm slm max** command to set the maximum number of number of sessions during which SLM frames are transmitted to a MEP.

### Examples

The following example shows how to set the amount of time to wait between sessions during which SLM frames are transmitted to a MEP. In this example, the amount of time to wait is 10 minutes.

```
Device> enable
Device# configure terminal
Device(config)# ethernet cfm slm max 1000
Device(config)# ethernet cfm slm timeout 10
```

### Related Commands

Command	Description
<b>ethernet cfm slm max</b>	Sets the maximum number of sessions during which SLM frames are transmitted to a MEP.

# ethernet cfm traceroute cache

To enable caching of Ethernet connectivity fault management (CFM) data learned through traceroute messages, use the **ethernet cfm traceroute cache** command in global configuration mode. To disable caching, use the **no** form of this command.

**ethernet cfm traceroute cache**  
**no ethernet cfm traceroute cache**

**Syntax Description** This command has no arguments or keywords.

**Command Default** Caching is disabled.

**Command Modes** Global configuration (config)

## Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SXI2	This command was integrated into Cisco IOS Release 12.2(33)SXI2.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
Cisco IOS 15.4(3)S	This command was implemented on Cisco ME 2600X Series Ethernet Access Switches.

**Usage Guidelines** Setting a traceroute cache allows you to store the results of traceroute operations initiated on the device.

**Examples** The following example shows how to enable Ethernet CFM traceroute cache:

```
Device(config)# ethernet cfm traceroute cache
```

## Related Commands

<b>ethernet cfm traceroute cache hold-time</b>	Sets a maximum time that Ethernet CFM traceroute cache entries will be retained.
<b>ethernet cfm traceroute cache size</b>	Sets a maximum number for entries in an Ethernet CFM traceroute cache table.

## ethernet cfm traceroute cache hold-time

To set the time that Ethernet connectivity fault management (CFM) traceroute cache entries are retained, use the **ethernet cfm traceroute cache hold-time** command in global configuration mode. To remove the configured time, use the **no** form of this command.

**ethernet cfm traceroute cache hold-time** *minutes*  
**no ethernet cfm traceroute cache hold-time**

<b>Syntax Description</b>	<i>minutes</i>	Integer in the range of 1 to 65535 that specifies the number of minutes that cache entries will be retained. The default is 100.
---------------------------	----------------	--

**Command Default** Entries are retained for 100 minutes.

**Command Modes** Global configuration (config)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(33)SRA	This command was introduced.
	12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
	12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
	12.2(33)SXI2	This command was integrated into Cisco IOS Release 12.2(33)SXI2.
	12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
	Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
	15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
	Cisco IOS 15.4(3)S	This command was implemented on Cisco ME 2600X Series Ethernet Access Switches.

**Usage Guidelines** Before you can issue this command, you must have enabled traceroute caching using the **ethernet cfm traceroute cache** command.

If traceroute cache is enabled and not empty and you change the hold time to less than the currently configured time, the change is rejected. You are prompted to clean up the table before the new hold time can be accepted. For example:

```
Device(config)# ethernet cfm traceroute cache hold-time 5
Please clean up the cache before setting smaller hold-time
current hold time = 100 Command Aborted.
Device(config)#
```

Output of the **show running all** command displays “ethernet cfm traceroute cache hold-time 100” when traceroute cache is enabled and the default value of 100 is configured.

---

**Examples**

The following example shows how to set the retention time for entries in an Ethernet CFM traceroute cache table to 5 minutes:

```
Device(config)# ethernet cfm traceroute cache hold-time 5
```

---

**Related Commands**

<b>ethernet cfm traceroute cache</b>	Enables caching of Ethernet CFM data learned from traceroute messages.
<b>ethernet cfm traceroute cache size</b>	Sets a maximum number for entries in an Ethernet CFM traceroute cache table.
<b>show running all</b>	Shows the running configuration with default values.

## ethernet cfm traceroute cache size

To set a maximum size for the Ethernet connectivity fault management (CFM) traceroute cache table, use the **ethernet cfm traceroute cache size** command in global configuration mode. To remove the configured size, use the **no** form of this command.

**ethernet cfm traceroute cache size** *entries*  
**no ethernet cfm traceroute cache size**

<b>Syntax Description</b>	<i>entries</i>	Number of entries in the traceroute cache table, expressed as an integer in the range of 1 to 4095. The default is 100.
---------------------------	----------------	---

**Command Default** If traceroute cache is enabled, traceroute replies are cached up to a maximum of 100 entries. If traceroute cache is disabled, traceroute replies are not cached; the default size is 0.

**Command Modes** Global configuration (config)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(33)SRA	This command was introduced.
	12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
	12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
	12.2(33)SXI2	This command was integrated into Cisco IOS Release 12.2(33)SXI2.
	12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
	Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
	15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
	Cisco IOS 15.4(3)S	This command was implemented on Cisco ME 2600X Series Ethernet Access Switches.

**Usage Guidelines** Before you can issue this command, you must have enabled traceroute caching using the **ethernet cfm traceroute cache** command.

Entries in the traceroute cache table are single replies from remote devices—not the number of operations on the device. In Cisco pre-Standard CFM Draft 1 when the maximum cache size is reached, new replies cannot be added until you clear the cache or increase its size. In CFM IEEE 802.1ag Standard when the maximum cache size is reached, the oldest traceroute operation is removed to make room for a new traceroute operation.

Output of the **show running all** command displays “ethernet cfm traceroute cache size 100” when traceroute cache is enabled and the default value of 100 is configured.

Setting the number of entries lower than the number of entries currently cached causes this command to be rejected, and you are prompted to clear the traceroute cache.

## Examples

The following example shows how to set the maximum number of entries in an Ethernet CFM traceroute cache table to 2500:

```
Device(config)# ethernet cfm traceroute cache size 2500
```

## Related Commands

Command	Description
<b>ethernet cfm traceroute cache</b>	Enables caching of Ethernet CFM data learned from traceroute messages.
<b>ethernet cfm traceroute cache hold-time</b>	Sets the maximum time that Ethernet CFM traceroute cache entries will be retained.
<b>show running all</b>	Shows the running configuration with default values.

## ethernet event microwave

To configure the settings of the Ethernet microwave event, use the **ethernet event microwave** command in interface configuration mode. To change the settings, use the **no** form of this command.

```
ethernet event microwave{hold-off seconds | loss-threshold number-of-messages | wtr seconds}
no ethernet event microwave{hold-off seconds | loss-threshold number-of-messages | wtr seconds}
```

Syntax Description		
<b>hold-off</b> <i>seconds</i>		Specifies the microwave bandwidth degradation hold-off time, in seconds. This time is used to prevent changes in the state of the network node as a result of signal degradation (SD) occurrences. Enter a number from 0 to 600. The default is 0.
<b>loss-threshold</b> <i>number-of-messages</i>		Specifies the number of bandwidth Vendor-Specific Messages (VSM) sent from the microwave transceiver to the Cisco device. Enter a number from 2 to 255. The default is 3.
<b>wtr</b> <i>seconds</i>		Specifies the wait-to-restore (wtr) time, in seconds. This time is used to prevent changes in the state of the network node as a result of recovery events after an SD occurrence. Enter a number from 0 to 600. The default is 10.

### Command Default

The settings for the Ethernet microwave event are not configured.

### Command Modes

Interface configuration (config-if)

### Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

### Usage Guidelines

Use the **event ethernet microwave sd interface threshold** command in applet configuration mode (config-applet) to create the Ethernet microwave event and use the **action switch ring g8032 instance** command to specify the G.8032 Ethernet ring protection (ERP) link and service instance in the ring topology. Then use the **ethernet event microwave** command in interface configuration mode (config-if) to configure the settings for the Ethernet microwave event, as applicable.

### Examples

The following example shows how to configure the settings for the Ethernet microwave event:

```
Device> enable
Device# configure terminal
Device(config)# event manager applet mw_ring_sd1
Device(config-applet)# event ethernet microwave sd interface gigabitethernet 0/0/0 threshold
400
Device(config-applet)# action 1 switch ring g8032 ringA instance 1
Device(config)# exit
Device(config)# interface gigabitethernet 0/0/0
Device(config-if)# ethernet event microwave hold-off 30
Device(config-if)# ethernet event microwave loss-threshold 100
Device(config-if)# ethernet event microwave wtr 45
Device(config)# end
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>action switch ring g8032 instance</b>	Specifies the protocol switch action for an instance on a link of a G.8032 ERP topology
<b>event ethernet microwave sd interface threshold</b>	Creates the Ethernet microwave event



# ethernet evc

To define an Ethernet virtual connection (EVC) and to enter EVC configuration mode, use the **ethernet evc** command in global configuration mode. To delete the EVC, use the **no** form of this command.

**ethernet evc** *evc-id*

**no ethernet evc** *evc-id*

<b>Syntax Description</b>	<i>evc-id</i> String from 1 to 100 characters that identifies the EVC.
---------------------------	--

**Command Default** No EVCs are defined.

**Command Modes** Global configuration (config)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(25)SEG	This command was introduced.
	12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
	12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.
	Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.
	15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

**Usage Guidelines** After you enter the **ethernet evc** command, the device enters EVC configuration mode and the following configuration commands are available:

- **default** -- Sets the EVC to its default states.
- **exit** -- Exits EVC configuration mode and returns the CLI to global configuration mode.
- **no** -- Negates a command or returns a command to its default setting.
- **oam protocol** -- Configures the Ethernet operations, administration, and maintenance (OAM) protocol and sets parameters.
- **uni count** -- Configures a UNI count for the EVC.

## Examples

The following example shows how to define an EVC named test1 and to enter EVC configuration mode:

```
Device(config)# ethernet evc test1
Device(config-enc)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>oam protocol</b>	Configures the EVC OAM protocol.
<b>service instance</b>	Configures an Ethernet service instance and attaches an EVC to it.
<b>show ethernet service evc</b>	Displays information about configured EVCs.
<b>uni count</b>	Sets the UNI count for an EVC.

# ethernet lmi

To set Ethernet local management interface (LMI) parameters for a user-network interface (UNI), use the **ethernet lmi** command in interface configuration mode. To remove Ethernet LMI parameters on a UNI, use the **no** form of this command.

**ethernet lmi** {**n391** | **n393** | **t391** | **t392**} *value*

**no ethernet lmi** {**n391** | **n393** | **t391** | **t392**}

## Syntax Description

<b>n391</b>	Polling counter on the customer equipment. A polling counter polls the status of the UNI and all Ethernet virtual connections (EVCs).
<b>n393</b>	An error counter for customer equipment or for a metro Ethernet network.
<b>t391</b>	Polling timer on the customer equipment. A polling timer transmits status enquiries and when status messages are not received, records errors.
<b>t392</b>	Polling verification timer on the metro Ethernet network. The polling verification timer verifies status enquiries received. When a timer expires, an error is recorded and the timer is restarted.  <b>Note</b> The t392 timer is valid only on Ethernet LMI provider edge (PE) devices. It is not available on customer edge (CE) devices.
<i>value</i>	Integer value within ranges that vary depending on the keyword with which it is used. Valid values are as follows: <ul style="list-style-type: none"> <li>• <b>n391</b> --1 to 65000. Default is 360.</li> <li>• <b>n393</b> --1 to 10. Default is 4.</li> <li>• <b>t391</b> --5 to 30 (seconds). Default is 10.</li> <li>• <b>t392</b> --5 to 30 (seconds); default is 15 or 0 to 0 (0-0), which disables the timer.</li> </ul>

## Command Default

Ethernet LMI parameters are not set on any UNIs.

## Command Modes

Interface configuration (config-if)

## Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(33)SRB	Support for this command on the Cisco 7600 router was integrated into Cisco IOS Release 12.2(33)SRB.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

## Usage Guidelines

The value for the polling verification timer (t392) should be greater than the value for the polling timer (t391).

The polling verification timer (t392) can be disabled.

A very high value for the polling timer (t391) means more time spent detecting Ethernet LMI link-down errors.

---

## Examples

The following example shows how to set a polling counter for 30 seconds on interface Ethernet 1/0:

```
Device# configure terminal  
Device(config)# interface ethernet 1/0  
Device(config-if)# ethernet lmi t391 30
```

# ethernet lmi ce-vlan map

To configure Ethernet Local Management Interface (LMI) parameters, use the **ethernet lmi ce-vlan map** command in Ethernet service configuration mode. To remove the configuration, use the **no** form of this command.

**ethernet lmi ce-vlan map** {*vlan-id* [**untagged**] | **any** | **default** | **untagged**};  
**no ethernet lmi ce-vlan map** {*vlan-id* | **any** | **default** | **untagged**};

Syntax Description	
<i>vlan-id</i>	Integer in the range of 1 to 4094 that identifies the customer VLAN or VLANs to map to. <ul style="list-style-type: none"> <li>You can enter a range of VLAN IDs using a hyphen (-) between IDs or enter a series of VLAN IDs using a comma (,) to separate each one.</li> </ul>
<b>untagged</b>	Map untagged VLANs. (Optional) When used with a range or series of VLANs, the <b>untagged</b> keyword is optional.
<b>any</b>	Map all VLANs (untagged and VLANs 1 to 4094).
<b>default</b>	Map to the default service instance. <ul style="list-style-type: none"> <li>You can use the <b>default</b> keyword only if you have already mapped the service instance to a VLAN or a group of VLANs.</li> </ul>

**Command Default** No Ethernet LMI mapping parameters are defined.

**Command Modes** Ethernet service configuration (config-if-srv)

Command History	Release	Modification
	12.2(25)SEG	This command was introduced.
	12.2(33)SRB	This command was implemented on the Cisco 7600 series routers.
	12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.
	Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

**Usage Guidelines** If you intend to use the **ethernet lmi ce-vlan map any** command, you must first configure all-to-one bundling on the interface.

This command can also be used to configure an Ethernet LMI customer VLAN-to-EVC map for a particular user-network interface (UNI).



**Note** To specify both VLAN IDs and untagged VLANs in the map, specify the VLAN IDs first and then specify the **untagged** keyword as follows: **ethernet lmi ce-vlan map 100,200,300,untagged**. Also, if the **untagged** keyword is not specified in the map configuration, the main interface line protocol on the Customer Edge (CE) device will be down.

Ethernet LMI mapping parameters are related to the bundling characteristics set by entering the **ethernet uni** command in interface configuration mode.

- Using the default UNI attribute (bundling and multiplexing) supports multiple EVCs and multiple VLANs.
- Entering the **ethernet uni bundle** command supports only one EVC with one or more VLANs.
- Entering the **ethernet uni bundle all-to-one** command supports multiple VLANs but only one EVC. If you use the **ethernet lmi ce-vlan map any** command in Ethernetservice configuration mode, you must first configure all-to-one bundling on the interface.
- Entering the **ethernet uni multiplex** command supports multiple EVCs with only one VLAN per EVC.

## Examples

The following example shows how to configure an Ethernet LMI customer VLAN-to-EVC map to test customer VLAN 101 in service instance 333 on the interface:

```
Device(config)# interface ethernet 2/1
Device(config-if)# service instance 333 ethernet test
Device(config-if-srv)# ethernet lmi ce-vlan map 101
```

## Related Commands

Command	Description
<b>service instance ethernet</b>	Defines an Ethernet service instance and enters Ethernet service configuration mode.
<b>show ethernet service instance</b>	Displays information about configured Ethernet service instances.

# ethernet lmi global

To enable Ethernet local management interface (LMI) functionality globally on a device, use the **ethernet lmi global** command in global configuration mode. To disable Ethernet LMI globally on a device, use the **no ethernet lmi global** form of this command.

**ethernet lmi global**  
**no ethernet lmi global**

**Syntax Description** This command has no arguments or keywords.

**Command Default** Ethernet LMI is disabled.

**Command Modes** Global configuration (config)

Command History	Release	Modification
	12.4(9)T	This command was introduced.
	12.2(33)SRB	Support for this command on the Cisco 7600 router was integrated into Cisco IOS Release 12.2(33)SRB.
	15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
	15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

**Usage Guidelines** Ethernet LMI is disabled by default on an interface and must be explicitly enabled. The **ethernet lmi global** command enables Ethernet LMI on all interfaces for an entire device. The benefit of this command is that you can enable Ethernet LMI on all interfaces with one command compared to enabling Ethernet LMI separately on each interface.

To disable Ethernet LMI on a specific interface after the **ethernet lmi global** command has been issued, the **no ethernet lmi interface** command must be issued on that interface.

The sequence in which the **ethernet lmi interface** and **ethernet lmi global** commands are issued is significant. The latest command issued overrides the prior command issued.

## Examples

The following example shows how to enable Ethernet LMI globally on a device:

```
Device(config)# ethernet lmi global
```

Related Commands	Command	Description
	<b>ethernet lmi interface</b>	Enables Ethernet LMI for a user-network interface.

# ethernet lmi interface

To enable Ethernet local management interface (LMI) on a user-network interface (UNI), use the **ethernet lmi interface** command in interface configuration mode. To remove Ethernet LMI on a UNI, use the **no** form of this command.

**ethernet lmi interface**  
**no ethernet lmi interface**

**Syntax Description** This command has no arguments or keywords.

**Command Default** Ethernet LMI parameters are not set on any UNIs.

**Command Modes** Interface configuration (config-if)

Release	Modification
12.4(9)T	This command was introduced.
12.2(33)SRB	Support for this command on the Cisco 7600 router was integrated into Cisco IOS Release 12.2(33)SRB.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

**Usage Guidelines** This command enables Ethernet LMI processing on an interface if the **ethernet lmi global** command has not been issued. When the **ethernet lmi global** command has been issued, Ethernet LMI is enabled on all interfaces. In this case, the **no ethernet lmi interface** command overrides the **ethernet lmi global** command and disables Ethernet LMI processing on the interface.

The sequence in which the commands are issued is significant. The latest command issued overrides the prior command issued.

## Examples

The following example shows how to enable Ethernet LMI on interface Ethernet 1/0:

```
Device# configure terminal
Device(config)# interface ethernet 1/0
Device(config-if)# ethernet lmi interface
```

Command	Description
<b>ethernet lmi global</b>	Enables Ethernet LMI functionality globally on a device.



# ethernet loopback local interface

To start and stop the Ethernet data-plane loopback session on the interface, use the **ethernet loopback local interface** command in privileged EXEC configuration mode.

**ethernet loopback** {start | stop} **local interface** [**interface ethernet** *interface-number*] [**service instance** *service-instance-id*] {**external** | **internal**} [*filtering-options*]

Syntax Description		
<b>start</b>		Starts the remote loopback operation.
<b>stop</b>		Stops the remote loopback operation.
<b>interface ethernet</b> <i>interface-number</i>		(Optional) Specifies the Ethernet interface on which to start or stop the Ethernet loopback.
<b>service instance</b> <i>service-instance-id</i>		(Optional) Configures the Ethernet service instance. Valid entries range from 1 to 4000.
<b>external</b>		Enables loopback of the traffic from the wire.
<b>internal</b>		Enables loopback of the traffic from the relay.
<i>filtering-options</i>		(Optional) Fields upon which filtering is performed. You can specify multiple values for the filtering-options argument.

**Command Default** Ethernet data-plane loopback is disabled.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 3.8S	This command was introduced.

**Usage Guidelines** The **ethernet loopback permit** command needs to be issued before the **ethernet loopback local interface** command.

**Examples** The following example shows how to start an Ethernet data-plane loopback session on the interface using the external keyword:

```
Device# ethernet loopback start local interface ethernet 2/0 external
```

Related Commands	Command	Description
	<b>ethernet loopback permit</b>	Configures an Ethernet data-plane loopback session on the interface
	<b>show ethernet loopback</b>	Displays information about the configuration of a device or interface and verifies that Ethernet data-plane loopback session is running.

# ethernet loopback permit

To configure an Ethernet data-plane loopback session on the interface, use the **ethernet loopback permit** command in interface configuration mode. To disable the Ethernet data-plane loopback session on the interface, use the **no** form of this command.

**ethernet loopback permit** {external | internal}[vlan *vlan-id*]

**no ethernet loopback permit** {external | internal}[vlan *vlan-id*]

## Syntax Description

<b>external</b>	Allows the activation of loopback of the traffic from the wire.
<b>internal</b>	Allows the activation of loopback of the traffic from the relay.
<b>vlan</b> <i>vlan-id</i>	(Optional) Specifies the VLAN ID. <ul style="list-style-type: none"> <li>• Use a hyphen (-) to specify a range of VLANs.</li> <li>• Use a comma (,) to specify more than one VLAN ID or VLAN range.</li> </ul>

## Command Default

Ethernet data-plane loopback is disabled. When a VLAN is not specified in the command, the packets with all VLAN tags and untagged packets are loopbacked.

## Command Modes

Interface configuration (config-if)

## Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

## Usage Guidelines

This **ethernet loopback permit** command needs to be issued before the **ethernet loopback local interface** command. If the destination MAC address is a broadcast or multicast MAC, for both external and internal loopback, the burned-in address (BIA) of the interface is used as the source MAC address for the packets sent back to the initiator. If the destination IP address is a broadcast or multicast IP address, for both facility and terminal loopback, the IP address of the interface is used as the source IP of the packets sent back to the initiator.

## Examples

The following example shows how to configure an Ethernet data-plane loopback session under the subinterface:

```
interface Ethernet3/0.1
encapsulation dot1q 3 second-dot1q any
ethernet loopback permit external
ethernet loopback permit internal
end
```

The following example shows the how to configure an Ethernet data-plane loopback session under the Ethernet flow points:

```
interface Ethernet2/0
service instance 4 ethernet evc3
```

```
encapsulation dot1q 100 second-dot1q 200
ethernet loopback permit external
ethernet loopback permit internal
!
```

The following example shows the how to configure an Ethernet data-plane loopback session using external VLANs 2 to10 on the interface:

```
Device(config)# interface ethernet 0/1
Device(config-if)# ethernet loopback permit external vlan 2-10
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>ethernet loopback local interface</b>	Starts and stops the Ethernet data-plane loopback session on the interface.
<b>show ethernet loopback</b>	Displays information about the configuration of a device or interface and verifies that Ethernet data-plane loopback session is running.

# ethernet mac-flush notification mirp

To send Multiple Service Instance ID (I-SID) Registration Protocol (MIRP) messages to the remote end when the standby Point of Attachment (PoA) becomes active and to specify that MIRP messages should be processed when they are received, use the **ethernet mac-flush notification mirp** command in global configuration mode. To disable the notifications and processing, use the **no** form of this command.

**ethernet mac-flush notification mirp** [*cos value*]  
**[no] ethernet mac-flush notification mirp** [*cos value*]

## Syntax Description

<b>cos</b> <i>value</i>	Specify the class-of-service (CoS) bit in the MIRP messages to be sent per system. The <i>value</i> can be a number from 1 to 7. The default is 7.
-------------------------	--

## Command Default

This command is enabled by default, and the CoS bit in the MIRP messages is 7.

## Command Modes

Global config (config#)

## Command History

Release	Modification
12.2(33)SRE	This command was introduced.

## Usage Guidelines

When the **ethernet mac-flush notification mirp** command is configured, you can enter the **no mac-flush notification mirp** command in the service instance configuration mode. However, when the **no ethernet mac-flush notification mirp** command is configured, enabling MIRP for an individual service instance by configuring **mac-flush notification mirp** in service instance configuration mode is not allowed.

The service instance configuration mode commands are automatically generated as a result of the global commands. Therefore, you can not enable MIRP for service instances when the global **no mac-flush notification mirp** command is configured.

## Examples

The following example shows how to configure class-of-service bit 5 for MAC-flush notification for an Ethernet service instance:

```
ethernet mac-tunnel virtual 1
  bridge domain 100
  service instance 1 ethernet
    encapsulation dot1ah isid 10000
    mac-flush notification mirp cos 5
```

## Related Commands

Command	Description
<b>service instance</b>	Configures an Ethernet service instance.

# ethernet mac limit action flooding disable

To prevent Layer 2 flooding for packets with unknown destination MAC addresses, use the **ethernet mac limit action flooding disable** command in global configuration mode. To allow this flooding, use the **no** form of this command.

**ethernet mac limit action flooding disable**  
**no ethernet mac limit action flooding disable**

**Syntax Description** This command has no arguments or keywords.

**Command Default** The flooding is allowed.

**Command Modes** Global configuration (config)

Release	Modification
15.3(1)S	This command was introduced.
Cisco IOS XE Release 3.8S.	This command was integrated into Cisco IOS XE Release 3.8S.

**Usage Guidelines** When a Layer 2 device receives a packet, the destination MAC address is examined and the device looks at the MAC address table. Each MAC address table contains information and attributes such as the following:

- MAC destination address
- Bridge-domain ID
- Interface type and number
- Service instance number
- Forwarding policy

If the system finds a match (for example, the MAC destination address), the packets are forwarded to the appropriate interface associated with the MAC destination address. If the system does not find a match, copies of the packets are forwarded to all interfaces in that bridge domain (except the source destination interface). This is known as “flooding.”

Eventually, the packet reaches the correct destination MAC address and that destination replies. This reply allows the system to learn that the MAC destination address belongs to a specific interface and an entry in the MAC address table is created. The next time a packet with that MAC destination address is received, the packet is simply forwarded to the correct interface.

However, there is a limit to the number of MAC destination address entries that can be included in the MAC address table. This is known as the MAC address limit. When this limit is reached, the system cannot learn the new destination. Thus, this destination will always be flooded, which results in system degradation. Use the **ethernet mac limit action flooding disable** command to prevent flooding the destination. If flooding is disabled, when the packet’s MAC address destination is unknown, the packet is discarded.

## Examples

The following example shows how to prevent Layer 2 flooding for packets with unknown destination MAC addresses.

```
Device> enable
Device# configure terminal
Device(config)# ethernet mac limit action flooding disable
```

# ethernet mac limit maximum addresses

To set the maximum number of MAC addresses that can be learned on the system, use the **ethernet mac limit maximum addresses** command in global configuration mode. To return to the default setting, use the **no** form of this command.

```
ethernet mac limit maximum addresses maximum-addresses
no ethernet mac limit maximum addresses [maximum-addresses]
```

<b>Syntax Description</b>	<i>maximum-addresses</i>	Maximum number of MAC addresses. The maximum varies by device.
---------------------------	--------------------------	--

**Command Default** The maximum number of MAC addresses allowed by the device.

**Command Modes** Global configuration (config)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	15.3(1)S	This command was introduced.
	Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

## Examples

The following example shows how to set the maximum number of MAC addresses to 1000:

```
Device> enable
Device# configure terminal
Device(config)# ethernet mac limit maximum addresses 1000
```

## ethernet mac-tunnel virtual

To configure a virtual MAC-in-MAC tunnel and place the command-line interface (CLI) into MAC-in-MAC tunnel configuration mode, use the **ethernet mac-tunnel virtual** command in global configuration mode. To remove the configured virtual MAC-in-MAC tunnel, use the **no** form of this command.

**ethernet mac-tunnel virtual** *tunnel-id*  
**no ethernet mac-tunnel virtual** *tunnel-id*

<b>Syntax Description</b>	<table border="1"> <tr> <td style="vertical-align: top;"><i>tunnel-id</i></td> <td>           Integer from 1 to 2147483647 that identifies the MAC-in-MAC tunnel.           <ul style="list-style-type: none"> <li>The upper limit may vary based on the platform.</li> </ul> </td> </tr> </table>	<i>tunnel-id</i>	Integer from 1 to 2147483647 that identifies the MAC-in-MAC tunnel. <ul style="list-style-type: none"> <li>The upper limit may vary based on the platform.</li> </ul>
<i>tunnel-id</i>	Integer from 1 to 2147483647 that identifies the MAC-in-MAC tunnel. <ul style="list-style-type: none"> <li>The upper limit may vary based on the platform.</li> </ul>		

**Command Default** No virtual MAC-in-MAC tunnels are configured.

**Command Modes** Global configuration (config)

<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.2(33)SRE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.2(33)SRE	This command was introduced.
Release	Modification				
12.2(33)SRE	This command was introduced.				

**Usage Guidelines** Multiple MAC tunnels with the same identifier cannot coexist on a single bridge.  
 In Cisco IOS Release 12.2(33)SRE, the platform upper limit for tunnel IDs is 4094.

**Examples** The following example shows how to configure a virtual MAC-in-MAC tunnel and place the CLI into MAC-in-MAC tunnel configuration mode:

```
Router> enable
Router# configure terminal
Router(config)# ethernet mac-tunnel virtual 100
Router(config-tunnel-minm)#
```



## ethernet oam

To enable Ethernet operations, maintenance, and administration (OAM) on an interface, use the **ethernet oam** command in interface configuration mode. To disable Ethernet OAM on an interface, use the **no** form of this command.

**ethernet oam** [{**max-rate** *oampdus* | **min-rate** *num-seconds* | **mode** {**active** | **passive**} | **timeout** *seconds*}]

**no ethernet oam** [{**max-rate** | **min-rate** | **mode** {**active** | **passive**} | **timeout**}]

### Syntax Description

<b>max-rate</b> <i>oampdus</i>	(Optional) Sets the maximum rate, in seconds, at which OAM protocol data units (PDUs) can be sent. The range is from 1 to 10. The default is 10.
<b>min-rate</b> <i>num-seconds</i>	(Optional) Sets the minimum rate, in seconds or milliseconds (ms), at which OAM PDUs are transmitted. The range is from 1 to 10 (in seconds) and 100 to 900 in ms. The value in ms must be specified in increments of 100.
<b>mode</b>	(Optional) Sets the OAM client mode.
<b>active</b>	(Optional) Sets the OAM client mode to active after the interface was previously placed in passive mode. Default OAM client mode is Active.
<b>passive</b>	(Optional) Sets the OAM client mode to passive. In passive mode, a device cannot initiate discovery, inquire about variables, or set loopback mode.
<b>timeout</b> <i>seconds</i>	(Optional) Specifies the amount of time, in seconds or milliseconds, after which a device declares its OAM peer to be nonoperational and resets the peer's state machine. The range is from 2 to 30 in seconds and 500 to 1900 in ms. The value in ms must be specified in increments of 100.

### Command Default

Ethernet OAM is disabled.

### Command Modes

Interface configuration (config-if)

### Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
15.1(2)SNG	This command was implemented on the Cisco ASR 900 Series Aggregation Services Router.

Release	Modification
15.3(2)S	This command was integrated into Cisco IOS Release 15.3(2)S. The range for <b>min-rate</b> <i>num-seconds</i> and <b>timeout</b> <i>seconds</i> keyword-argument pairs was modified. The range for <i>num-seconds</i> was modified to 1 to 10 (in seconds) and 100 to 900 in ms. The range for <i>seconds</i> was modified to 2 to 30 in seconds and 500 to 1900 in ms. The value in ms must be specified in increments of 100.

### Usage Guidelines

When Ethernet OAM is configured on an interface, the default mode of the OAM client is active. When the Ethernet OAM mode is enabled on two interfaces passing traffic, both interfaces cannot be in passive mode. Both interfaces can be in active mode, and one can be in active mode and the other in passive mode. You can toggle between Ethernet OAM modes without disabling OAM.

The **min-rate** *num-seconds* keyword and argument pair controls the minimum rate, in seconds at which OAM PDUs can be sent on an interface. A value of *n*, where 1 is less than or equal to *n* and *n* is less than or equal to 10, indicates that an OAM PDU must be sent at least once per *n* seconds. If no other OAM PDU is to be sent within an *n*-second window, an information OAM PDU must be sent.

### Examples

The following example shows how to activate an Ethernet OAM interface that was previously configured to be in passive mode:

```
Device(config)# interface gigabitethernet 0/1
Device(config-if)# ethernet oam mode active
```

The following example shows how to set the maximum OAM PDUs transmission rate of 5 seconds on interface GigabitEthernet 0/1:

```
Device(config)# interface gigabitethernet 0/1
Device(config-if)# ethernet oam max-rate 5
```

The following example shows how to set the minimum OAM PDUs transmission rate of 500 ms on interface GigabitEthernet 0/1:

```
Device(config)# interface gigabitethernet 0/1
Device(config-if)# ethernet oam min-rate 500
```

The following example shows how to set the timeout period to 25 seconds on interface GigabitEthernet 0/1:

```
Device(config)# interface gigabitethernet 0/1
Device(config-if)# ethernet oam timeout 25
```

### Related Commands

Command	Description
<b>show ethernet cfm maintenance-points local</b>	Displays information about maintenance points configured on a device.
<b>show ethernet cfm maintenance-points remote crosscheck</b>	Displays information about remote maintenance points configured statically in a cross-check list.
<b>show ethernet cfm maintenance-points remote detail</b>	Displays information about a remote maintenance point in the continuity check database.

Command	Description
show ethernet oam status	Displays Ethernet OAM configurations for an interface.

# ethernet oam link-monitor frame

To configure an error frame threshold or window on an Ethernet operations, maintenance, and administration (OAM) interface, use the **ethernet oam link-monitor frame** command in configuration template mode or interface configuration mode. To remove the threshold or window, use the **no** form of this command.

**ethernet oam link-monitor frame** {**threshold** {**high** {**none***high-frames*} | **low** *low-frames*} | **window** *milliseconds*}

**no ethernet oam link-monitor frame** {**threshold** {**high** | **low**} | **window**}

## Syntax Description

<b>threshold</b>	Sets a number of error frames at, above, or below which an action is triggered.
<b>high</b>	Sets a high error frame threshold in number of frames.
<b>none</b>	Disables a high threshold.
<i>high-frames</i>	Integer in the range of 1 to 65535 that is the high threshold in number of frames.
<b>low</b>	Sets a low error frame threshold.
<i>low-frames</i>	Integer in the range of 0 to 65535 that sets the low threshold in number of frames. The default is 1.
<b>window</b>	Sets a window and period of time during which error frames are counted.
<i>milliseconds</i>	Integer in the range of 10 to 600 that represents a number of milliseconds in a multiple of 100. The default is 100.

## Command Default

The **ethernet oam link-monitor frame** command is not configured.

## Command Modes

Configuration template (config-template) Interface configuration (config-if)

## Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

## Usage Guidelines

The **ethernet oam link-monitor frame** command configures a number of error frames that triggers an action or a period of time in which error frames are counted.

## Examples

The following example shows how to configure an Ethernet OAM link-monitor frame window of 3000 milliseconds:

```
Device(config-template)# ethernet oam link-monitor frame window 300
```

**Related Commands**

<b>ethernet oam link-monitor frame-period</b>	Configures an error frame period on an Ethernet OAM interface.
<b>ethernet oam link-monitor frame-seconds</b>	Configures a frame-seconds period on an Ethernet OAM interface.
<b>ethernet oam link-monitor high-threshold action</b>	Configures a specific action to occur when a high threshold for an error is exceeded on an Ethernet OAM interface.
<b>ethernet oam link-monitor receive-crc</b>	Configures an Ethernet OAM interface to monitor frames received with CRC errors for a period of time.
<b>ethernet oam link-monitor symbol-period</b>	Configures an error symbol period on an Ethernet OAM interface.
<b>ethernet oam link-monitor transmit-crc</b>	Configures an Ethernet OAM interface to monitor frames transmitted with CRC errors for a period of time.

# ethernet oam link-monitor frame-period

To configure an error frame period on an Ethernet operations, maintenance, and administration (OAM) interface, use the **ethernet oam link-monitor frame-period** command in configuration template or interface configuration mode. To remove the frame period, use the **no** form of this command.

**ethernet oam link-monitor frame-period** {**threshold** {**high** {*none**high-frames*} | **low** *low-frames*} | **window** *frames*}

**no ethernet oam link-monitor frame-period** {**threshold** {**high** | **low**} | **window**}

## Syntax Description

<b>threshold</b>	Sets a number of error frames for the period at, above, or below which an action is triggered.
<b>high</b>	Sets a high threshold for the error frame period in number of frames.
<b>none</b>	Disables a high threshold.
<i>high-frames</i>	Integer in the range of 1 to 65535 that is the high threshold in number of frames. There is no default. The high threshold must be configured.
<b>low</b>	Sets a low threshold for the error frame period in number of frames.
<i>low-frames</i>	Integer in the range of 0 to 65535 that is the low threshold in number of frames. The default is 1.
<b>window</b>	Sets a polling window and window size.
<i>frames</i>	Integer in the range of 1 to 65535 that is the window size in number of frames. Each value is a multiple of 10000. The default is 1000.

## Command Default

An error frame period on an Ethernet OAM interface is not configured.

## Command Modes

Configuration template (config-template)

Interface configuration (config-if)

## Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

## Usage Guidelines

The **ethernet oam link-monitor frame-period** command configures an error frame period in number of frames. When a high threshold is configured, it must be at least as great as the low threshold for frame errors.

The number of frames polled is user defined. Note that the system can poll only by time, not by frames. The number of frames you specify is converted internally to seconds using a formula that includes interface speed.

## Examples

The following example shows how to configure an Ethernet OAM link-monitor frame-period window of 20000 frames:

```
Device(config-template)# ethernet oam link-monitor frame-period window 2
```

The following example shows how to configure an Ethernet OAM link-monitor frame-period low threshold of 500 frames:

```
Device(config-template)# ethernet oam link-monitor frame-period threshold low 500
```

## Related Commands

<b>ethernet oam link-monitor frame</b>	Configures an error frame threshold or window on an Ethernet OAM interface.
<b>ethernet oam link-monitor frame-seconds</b>	Configures a frame-seconds period on an Ethernet OAM interface.
<b>ethernet oam link-monitor high-threshold action</b>	Configures a specific action to occur when a high threshold for an error is exceeded on an Ethernet OAM interface.
<b>ethernet oam link-monitor receive-crc</b>	Configures an Ethernet OAM interface to monitor frames received with CRC errors for a period of time.
<b>ethernet oam link-monitor symbol-period</b>	Configures an error symbol period on an Ethernet OAM interface.
<b>ethernet oam link-monitor transmit-crc</b>	Configures an Ethernet OAM interface to monitor frames transmitted with CRC errors for a period of time.

## ethernet oam link-monitor frame-seconds

To configure a frame-seconds period on an Ethernet operations, maintenance, and administration (OAM) interface, use the **ethernet oam link-monitor frame-seconds** command in configuration template and interface configuration mode. To remove the threshold or window, use the **no** form of this command.

```
ethernet oam link-monitor frame-seconds {threshold {high {nonehigh-frames} | low low-frames}
| window milliseconds}
```

```
no ethernet oam link-monitor frame-seconds {threshold {high | low} | window}
```

### Syntax Description

<b>threshold</b>	Sets a number at, above, or below which an action is triggered.
<b>high</b>	Sets a high error frame-seconds threshold in number of seconds.
<b>none</b>	Disables a high threshold.
<i>high-frames</i>	Integer in the range of 1 to 900 that is the high threshold in number of frames. There is no default. The high threshold must be configured.
<b>low</b>	Sets a low error frame-seconds threshold in number of seconds.
<i>low-frames</i>	Integer in the range of 1 to 900 that sets the low threshold in number of frames. The default is 1.
<b>window</b>	Sets a polling window during which error frames are counted.
<i>milliseconds</i>	Integer in the range of 100 to 9000 that represents a number of milliseconds in a multiple of 100. The default is 1000.

### Command Default

A frame-seconds period on an Ethernet OAM interface is not configured.

### Command Modes

Configuration template (config-template)

Interface configuration (config-if)

### Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

### Usage Guidelines

The **ethernet oam link-monitor frame-seconds** command configures a number of error frames that triggers an action or a period of time in which error frames are counted.



**Examples**

The following example shows how to configure an Ethernet OAM link-monitor frame-seconds window of 30000 milliseconds (30 seconds):

```
Device(config-template)# ethernet oam link-monitor frame-seconds window 300
```

**Related Commands**

<b>ethernet oam link-monitor frame</b>	Configures an error frame threshold or window on an Ethernet OAM interface.
<b>ethernet oam link-monitor frame-period</b>	Configures an error frame period on an Ethernet OAM interface.
<b>ethernet oam link-monitor high-threshold action</b>	Configures a specific action to occur when a high threshold for an error is exceeded on an Ethernet OAM interface.
<b>ethernet oam link-monitor receive-crc</b>	Configures an Ethernet OAM interface to monitor frames received with CRC errors for a period of time.
<b>ethernet oam link-monitor symbol-period</b>	Configures an error symbol period on an Ethernet OAM interface.
<b>ethernet oam link-monitor transmit-crc</b>	Configures an Ethernet OAM interface to monitor frames transmitted with CRC errors for a period of time.

# ethernet oam link-monitor high-threshold action

To configure a specific action to occur when a high threshold for an error is exceeded on an Ethernet operations, maintenance, and administration (OAM) interface, use the **ethernet oam link-monitor high-threshold action** command in configuration template mode. To remove the high-threshold action, use the **no** form of this command.

**ethernet oam link-monitor high-threshold action** {**error-disable-interface** | **failover**}

**no ethernet oam link-monitor high-threshold action**

## Syntax Description

<b>error-disable-interface</b>	Performs an error-disable function on the interface.
<b>failover</b>	Performs a failover to another port in the same PortChannel.

## Command Default

A high-threshold action is not configured.

## Command Modes

Configuration template (config-template)

## Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

## Usage Guidelines

The failover action is applicable only to EtherChannel interfaces. It provides an automatic failover of traffic from one port in an EtherChannel to another port in the same EtherChannel when one of the ports in the channel exceeds the high threshold for an error within the specified interval. The port failover occurs only if at least one operational port is in the EtherChannel. The failed port is put into an error-disable state. If the failed port is the last port in the EtherChannel, the port will not be put into the error-disable state and will continue to pass traffic regardless of the types of errors received.

Single, nonchanneling ports go into the error-disable state when the error high threshold is exceeded within the specified interval.

## Examples

The following example shows how to configure an error-disable-interface action to occur when the high threshold for an error is exceeded:

```
Device(config-template)# ethernet oam link-monitor high-threshold action
error-disable-interface
```

**Related Commands**

<b>ethernet oam link-monitor frame</b>	Configures an error frame threshold or window on an Ethernet OAM interface.
<b>ethernet oam link-monitor frame-period</b>	Configures an error frame period on an Ethernet OAM interface.
<b>ethernet oam link-monitor frame-seconds</b>	Configures a frame-seconds period on an Ethernet OAM interface.
<b>ethernet oam link-monitor receive-crc</b>	Configures an Ethernet OAM interface to monitor frames received with CRC errors for a period of time.
<b>ethernet oam link-monitor symbol-period</b>	Configures an error symbol period on an Ethernet OAM interface.
<b>ethernet oam link-monitor transmit-crc</b>	Configures an Ethernet OAM interface to monitor frames transmitted with CRC errors for a period of time.

# ethernet oam link-monitor on

To enable link monitoring on an Ethernet operations, maintenance, and administration (OAM) interface, use the **ethernet oam link-monitor on** command in interface configuration mode. To disable link monitoring, use the **no** form of this command.

**ethernet oam link-monitor on**

**no ethernet oam link-monitor on**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Link monitoring is turned on when Ethernet OAM is enabled.

## Command Modes

Interface configuration (config-if)

## Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

## Usage Guidelines

When link monitoring is enabled, the interface sends event OAM protocol data units (PDUs) when errors occur and interprets event OAM PDUs from the remote peer. Link monitoring can be effective only if both the local client and remote peer agree to support it.

The **ethernet oam link-monitor on** command is enabled by default when Ethernet OAM is enabled and does not display in the configuration when the **show running-config** command is issued.

When link monitoring is enabled by default, to turn it off you must explicitly disable it by issuing the **no** form of this command.

## Examples

The following example shows how to disable link monitoring on Ethernet OAM interface Ethernet 0/1:

```
Device(config)# interface ethernet 0/1
Device(config-if)# no
ethernet oam link-monitor on
```

## Related Commands

<b>ethernet oam link-monitor supported</b>	Enables support for link monitoring on an Ethernet OAM interface.
--	---

## ethernet oam link-monitor receive-crc

To configure an Ethernet operations, maintenance, and administration (OAM) interface to monitor ingress frames received with cyclic redundancy code (CRC) errors for a period of time, use the **ethernet oam link-monitor receive-crc** command in configuration template or interface configuration mode. To disable monitoring, use the **no** form of this command.

```
ethernet oam link-monitor receive-crc {threshold {high {high-frames | none} | low low-frames} | window milliseconds}
```

```
no ethernet oam link-monitor receive-crc {threshold {high | low} | window}
```

### Syntax Description

<b>threshold</b>	Sets a number of frames with CRC errors received at, above, or below which an action is triggered.
<b>high</b>	Sets a high threshold in number of frames.
<i>high-frames</i>	Integer in the range of 1 to 65535 that is the high threshold in number of frames.
<b>none</b>	Disables a high threshold.
<b>low</b>	Sets a low threshold.
<i>low-frames</i>	Integer in the range of 0 to 65535 that sets the low threshold in number of frames. The default is 10.
<b>window</b>	Sets a window and period of time during which frames with CRC errors are counted.
<i>milliseconds</i>	Integer in the range of 10 to 1800 that represents a number of milliseconds in a multiple of 100. The default is 1000.

### Command Default

The **ethernet oam link-monitor receive-crc** command is not configured.

### Command Modes

Configuration template (config-template) Interface configuration (config-if)

### Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

### Usage Guidelines

OAM must be operational on the interface before you issue this command.

**Examples**

The following example shows how to configure a receive-crc period with a low threshold of 3000:

```
Device(config-if)# ethernet oam link-monitor receive-crc threshold low 3000
```

**Related Commands**

<b>ethernet oam link-monitor frame</b>	Configures an error frame threshold or window on an Ethernet OAM interface.
<b>ethernet oam link-monitor frame-period</b>	Configures an error frame period on an Ethernet OAM interface.
<b>ethernet oam link-monitor frame-seconds</b>	Configures a frame-seconds period on an Ethernet OAM interface.
<b>ethernet oam link-monitor high-threshold action</b>	Configures a specific action to occur when a high threshold for an error is exceeded on an Ethernet OAM interface.
<b>ethernet oam link-monitor symbol-period</b>	Configures an error symbol period on an Ethernet OAM interface.
<b>ethernet oam link-monitor transmit-crc</b>	Configures an Ethernet OAM interface to monitor frames transmitted with CRC errors for a period of time.

# ethernet oam link-monitor supported

To enable support for link monitoring on an Ethernet operations, maintenance, and administration (OAM) interface, use the **ethernet oam link-monitor supported** command in interface configuration mode. To disable link monitoring support, use the **no** form of this command.

**ethernet oam link-monitor supported**  
**no ethernet oam link-monitor supported**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Link monitoring is supported when Ethernet OAM is enabled.

## Command Modes

Interface configuration (config-if)

## Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

## Usage Guidelines

Use this command to help establish an OAM session for performing OAM functions, such as remote loopback. For example, if your device is connected to a third-party device that does not support link monitoring, you must disable link monitoring support on your device to establish an OAM session with the third-party device.

When the **ethernet oam link-monitor supported** command has been issued, remote loopback will not function, whether or not an interface has been configured to support it.

The **ethernet oam link-monitor supported** command is enabled by default when Ethernet OAM is enabled and does not display in the configuration when the **show running-config** command is issued.

When support for link monitoring is enabled by default, to turn it off you must explicitly disable it by issuing the **no** form of this command.

## Examples

The following example shows how to disable support for link monitoring on the GigabitEthernet 0/1 OAM interface:

```
Device(config)# interface gigabitethernet 0/1
Device(config-if)# no ethernet oam link-monitor supported
```

The following example shows how to reenable support for link monitoring on the GigabitEthernet 0/1 OAM interface after support has been disabled:

```
Device(config)# interface gigabitethernet 0/1  
Device(config-if)# ethernet oam link-monitor supported
```

**Related Commands**

<b>ethernet oam link-monitor on</b>	Enables link monitoring on an Ethernet OAM interface.
-------------------------------------	---



## ethernet oam link-monitor symbol-period

To configure an error symbol period on an Ethernet operations, maintenance, and administration (OAM) interface, use the **ethernet oam link-monitor symbol-period** command in configuration template or interface configuration mode. To remove the symbol period, use the **no** form of this command.

**ethernet oam link-monitor symbol-period** {**threshold** {**high** {**none***high-symbols*} | **low** *low-symbols*} | **window** *symbols*}

**no ethernet oam link-monitor symbol-period** {**threshold** {**high** | **low**} | **window**}

### Syntax Description

<b>threshold</b>	Sets a number of error symbols at, above, or below which an action is triggered.
<b>high</b>	Sets a high threshold for the period in number of error symbols.
<b>none</b>	Disables a high threshold.
<i>high-symbols</i>	Integer in the range of 1 to 65535 that is the high threshold in number of symbols. There is no default. The high threshold must be configured.
<b>low</b>	Sets a low threshold for the period in number of error symbols.
<i>low-symbols</i>	Integer in the range of 0 to 65535 that is the low threshold in number of symbols.
<b>window</b>	Sets a window and window size.
<i>symbols</i>	Integer in the range of 1 to 65535 that is the window size in number of symbols. Each value represents one million.

### Command Default

The **ethernet oam link-monitor symbol-period** command is not configured.

### Command Modes

Configuration template (config-template) Interface configuration (config-if)

### Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.

### Usage Guidelines

The **ethernet oam link-monitor symbol-period** command configures an error symbol threshold or error symbol window in number of symbols. When a high threshold is configured, it must be at least as great as the low threshold for symbol errors.

This command can be applied to an Ethernet OAM template and to an interface. The value configured on an interface takes precedence over the value configured by this command for the template.

This command is prefixed with “ether oam” in interface configuration mode.

**Examples**

The following example shows how to configure a symbol-period window of 500 million error symbols:

```
Device(config-template)# ethernet oam link-monitor symbol-period window 500
```

The following example shows how to configure a symbol-period low threshold of 500 error symbols:

```
Device(config-template)# ethernet oam link-monitor symbol-period threshold low 500
```

**Related Commands**

<b>ethernet oam link-monitor frame</b>	Configures an error frame threshold or window on an Ethernet OAM interface.
<b>ethernet oam link-monitor frame-period</b>	Configures an error frame period on an Ethernet OAM interface.
<b>ethernet oam link-monitor frame-seconds</b>	Configures a frame-seconds period on an Ethernet OAM interface.
<b>ethernet oam link-monitor high-threshold action</b>	Configures a specific action to occur when a high threshold for an error is exceeded on an Ethernet OAM interface.
<b>ethernet oam link-monitor receive-crc</b>	Configures an Ethernet OAM interface to monitor frames received with CRC errors for a period of time.
<b>ethernet oam link-monitor transmit-crc</b>	Configures an Ethernet OAM interface to monitor frames transmitted with CRC errors for a period of time.

## ethernet oam link-monitor transmit-crc

To configure an Ethernet operations, maintenance, and administration (OAM) interface to monitor egress frames transmitted with cyclic redundancy code (CRC) errors for a period of time, use the **ethernet oam link-monitor transmit-crc** command in configuration template or interface configuration mode. To disable monitoring, use the **no** form of this command.

```
ethernet oam link-monitor transmit-crc {threshold {high {high-frames | none} | low low-frames}
| window milliseconds}
```

```
no ethernet oam link-monitor transmit-crc {threshold {high | low} | window}
```

### Syntax Description

<b>threshold</b>	Sets a number of frames with CRC errors transmitted at, above, or below which an action is triggered.
<b>high</b>	Sets a high threshold in number of frames.
<i>high-frames</i>	Integer in the range of 1 to 65535 that is the high threshold in number of frames.
<b>none</b>	Disables a high threshold.
<b>low</b>	Sets a low threshold.
<i>low-frames</i>	Integer in the range of 0 to 65535 that sets the low threshold in number of frames. The default is 10.
<b>window</b>	Sets a window and period of time during which frames with transmit CRC errors are counted.
<i>milliseconds</i>	Integer in the range of 10 to 1800 that represents a number of milliseconds in a multiple of 100. The default is 100.

### Command Default

An Ethernet OAM interface to monitor egress frames transmitted with CRC errors for a period of time is not configured.

### Command Modes

Configuration template (config-template)

Interface configuration (config-if)

### Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

**Usage Guidelines**

OAM must be operational on the interface before you issue this command.

**Examples**

The following example shows how to configure a transmit CRC window of 2500 milliseconds:

```
Device(config-if)# ethernet oam link-monitor transmit-crc window 25
```

**Related Commands**

<b>ethernet oam link-monitor frame</b>	Configures an error frame threshold or window on an Ethernet OAM interface.
<b>ethernet oam link-monitor frame-period</b>	Configures an error frame period on an Ethernet OAM interface.
<b>ethernet oam link-monitor frame-seconds</b>	Configures a frame-seconds period on an Ethernet OAM interface.
<b>ethernet oam link-monitor high-threshold action</b>	Configures a specific action to occur when a high threshold for an error is exceeded on an Ethernet OAM interface.
<b>ethernet oam link-monitor receive-crc</b>	Configures an Ethernet OAM interface to monitor frames received with CRC errors for a period of time.
<b>ethernet oam link-monitor symbol-period</b>	Configures an error symbol period on an Ethernet OAM interface.

# ethernet oam mib log size

To set the size of the Ethernet Operations, Administration, and Maintenance (OAM) event log table, use the **ethernet oam mib log size** command in global configuration mode. To remove the event log table, use the **no** form of this command.

**ethernet oam mib log size** *entries*  
**no ethernet oam mib log size**

<b>Syntax Description</b>	<i>entries</i>	Number of entries that the event log table will hold. Integer from 0 to 200. The minimum is 0, the maximum is 200, and the default is 50.
---------------------------	----------------	---

**Command Default** An event log table is not configured.

**Command Modes** Global configuration (config)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(33)SRD	This command was introduced.
	12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
	Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.
	15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

**Usage Guidelines** Use this command to configure an OAM event log table.

**Examples** The following example shows how to set the size of an event log table to 100 entries:

```
Device# configure terminal
Device(config)# ethernet oam mib log size 100
```

## ethernet oam remote-failure

To enable Ethernet Operations, Administration, and Maintenance (OAM) remote failure actions, use the **ethernet oam remote-failure** command in interface configuration mode. To disable Ethernet OAM remote failure actions, use the **no** form of this command.

**ethernet oam remote-failure** { **critical-event** | **dying-gasp** | **link-fault** } **action error-disable-interface**  
**no ethernet oam remote-failure** { **critical-event** | **dying-gasp** | **link-fault** } **action error-disable-interface**

### Syntax Description

<b>critical-event</b>	Specifies remote critical event failures.
<b>dying-gasp</b>	Specifies remote dying gasp failures.
<b>link-fault</b>	Specifies remote link fault failures.
<b>action</b>	Specifies the action that must be performed for the specified interface when an Ethernet OAM remote failure event occurs.
<b>error-disable-interface</b>	Disables the interface when an error occurs.

### Command Default

If Ethernet OAM remote failures occur, no action is performed.

### Command Modes

Interface configuration (config-if)

### Command History

Release	Modification
12.4(15)T	This command was introduced.
12.2(33)SRD	This command was integrated into Cisco IOS Release 12.2(33)SRD.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.3S	This command was integrated into a release earlier than Cisco IOS XE Release 2.3S.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
Cisco IOS XE Release 3.10S	This command was implemented on the Cisco ASR 903 Series Aggregation Services Router in a release earlier than Cisco IOS XE Release 3.10S.

### Usage Guidelines

When the **ethernet oam remote-failure** command is configured for an interface, the interface is automatically disabled when an Ethernet OAM remote failure event occurs.

### Examples

The following example shows how to disable the Ethernet interface 1/1 when a critical event failure occurs:

```
Device# configure terminal
Device(config)# interface ethernet 1/1
Device(config-if)# ethernet oam remote-failure critical-event action error-disable-interface
```

```
Device(config-if)# end
```

The following example shows how to disable the Gigabitethernet interface 0/1/0 when a link fault failure occurs:

```
Device# configure terminal
Device(config)# interface gigabitethernet 0/1/0
Device(config-if)# ethernet oam remote-failure link-fault action error-disable-interface
Device(config-if)# end
```

#### Related Commands

Command	Description
<b>ethernet oam</b>	Enables Ethernet OAM on an interface.

# ethernet oam remote-loopback

To turn on or off Ethernet operations, maintenance, and administration (OAM) remote loopback functionality on an interface, use the **ethernet oam remote-loopback** command in privileged EXEC mode. This command does not have a **no** form.

**ethernet oam remote-loopback** {start | stop} **interface** *type number*

## Syntax Description

<b>start</b>	Starts the remote loopback operation.
<b>stop</b>	Stops the remote loopback operation.
<b>interface</b>	Specifies an interface.
<i>type</i>	Type of Ethernet interface. Valid values are: FastEthernet, GigabitEthernet, TenGigabitEthernet.
<i>number</i>	Integer from 1 to 9 that is the number of the Ethernet interface.

## Command Default

Remote loopback functionality is turned off.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

## Usage Guidelines

A **no** form of this command is not available.

When Ethernet OAM remote loopback functionality is enabled on an interface, traffic sent out on this interface will be discarded or sent back (and dropped locally) by the remote interface.

Remote loopback will not function, whether or not an interface has been configured to support it, when the **no ethernet oam link-monitor supported** command has been issued.



**Note** To start Ethernet OAM remote loopback on a switch port, you must first configure the **access-group mode prefer port** command in interface configuration mode.

## Examples

The following example shows how to start a remote loopback session on interface GigabitEthernet 2/1:



```
Device# ethernet oam remote-loopback start interface gigabitethernet2/1
```

**Related Commands**

<b>access-group mode prefer port</b>	Specifies the override modes and the nonoverride modes for an access group and specifies that the ACL mode takes precedence if ACLs are configured.
<b>ethernet oam remote-loopback (interface)</b>	Enables the support of Ethernet OAM remote loopback operation on an interface or sets a remote loopback timeout period.

## ethernet oam remote-loopback (interface)

To enable the support of Ethernet operations, maintenance, and administration (OAM) remote loopback operations on an interface or set a remote loopback timeout period, use the **ethernet oam remote-loopback (interface)** command in interface configuration mode. To disable support or remove the timeout setting, use the **no** form of this command.

**ethernet oam remote-loopback** {supported | timeout *seconds*}

**no ethernet oam remote-loopback** {supported | timeout}

### Syntax Description

<b>supported</b>	Supports the remote loopback functionality.
<b>timeout</b>	Sets a primary loopback timeout setting.
<i>seconds</i>	Integer from 1 to 10 that is the number of seconds of the timeout period.

### Command Default

Remote loopback is not supported.

### Command Modes

Interface configuration (config-if)

### Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

### Usage Guidelines

This command enables the support of OAM remote-loopback on an interface. Only after this functionality is enabled can the local OAM client initiate the OAM remote loopback operation. Changing this setting causes the local OAM client to exchange configuration information with its remote peer.

The **no** form of the command is rejected if the interface is in the loopback mode.



**Note** To start Ethernet OAM remote loopback on a switch port, you must first configure the **access-group mode prefer port** command in interface configuration mode.

### Examples

The following example shows how to enable remote loopback support on interface GigabitEthernet 2/1:

```
Device(config)# interface gigabitethernet 2/1
Device(config-if)# ethernet oam remote-loopback supported
```

**Related Commands**

<b>access-group mode prefer port</b>	Specifies the override modes and the nonoverride modes for an access group and specifies that the PAACL mode takes precedence if PAACLs are configured.
<b>ethernet oam remote-loopback</b>	Turns on or off the remote loopback functionality.

## ethernet ring g8032

To create an Ethernet ring, use the **ethernet ring g8032** command in global configuration mode. To remove the Ethernet ring, use the **no** form of this command.

```
ethernet ring g8032 ring-name
no ethernet ring g8032 ring-name
```

### Syntax Description

<i>ring-name</i>	Ethernet ring name no longer than 32 characters.
------------------	--

### Command Default

The Ethernet ring is not created.

### Command Modes

Global configuration (config)

### Command History

Release	Modification
Cisco IOS XE Release 3.6S	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

### Usage Guidelines

This command also enters Ethernet ring configuration mode (config-erp-ring).

### Examples

The following is an example of the **ethernet ring g8032** command used in an Ethernet ring configuration.

```
Device>enable
Device# configure terminal
Device(config)# ethernet ring g8032 ring1
Device(config-erp-ring)#
```

# ethernet ring g8032 profile

To create an Ethernet ring profile, use the **ethernet ring g8032 profile** command in global configuration mode. To delete the Ethernet ring profile, use the **no** form of this command.

```
ethernet ring g8032 profile profile-name
no ethernet ring g8032 profile profile-name
```

<b>Syntax Description</b>	<i>profile-name</i>	Ethernet ring profile name no longer than 32 characters.
---------------------------	---------------------	--

**Command Default** The Ethernet ring profile is not created.

**Command Modes** Global configuration (config)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 3.6S	This command was introduced.
	15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
	15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

**Usage Guidelines** This command also enters Ethernet ring profile configuration mode (config-erp-profile).

**Examples** The following is an example of the **ethernet ring g8032 profile** command used in an Ethernet ring configuration.

```
Device# configure
Device(config)# ethernet ring g8032 profile profile1
Device(config-erp-profile)#
```

# ethernet subscriber

To enable Ethernet Layer 2 (L2) context, use the **ethernetsubscriber** command in service instance configuration mode. To disable this command, use the **no** form of this command.

**ethernet subscriber**  
**no ethernet subscriber**

**Syntax Description** This command has no arguments or keywords.

**Command Default** Ethernet L2 context is not enabled.

**Command Modes** Service instance configuration (config-if-srv)

Command History	Release	Modification
	15.1(2)S	This command was introduced.

**Usage Guidelines** Before configuring the **ethernetsubscriber** command, you must configure the **encapsulation** command under a service instance. Else, you cannot enable the Ethernet L2 context. When you disable the **encapsulation** command, the **ethernetsubscriber** command is also disabled.

You can use the **ethernetsubscriber** command in service instance configuration mode to enable an Ethernet L2 context. The Ethernet L2 context is used to define the control plane policy for detecting first sign of life (FSOL).

Configuring this command on any platform indicates that the unclassified traffic on the specific service instance will not be dropped; instead, it will be punted to the FSOL handling mechanism.

## Examples

The following example shows how to enable an Ethernet L2 context:

```
Router# configure terminal
Router(config)# interface GigabitEthernet 1/25
Router(config-if)# service instance dynamic 1 ethernet
Router(config-if-srv)# encapsulation dot1q 200

Router(config-if-srv)# ethernet subscriber
```

Related Commands	Command	Description
	<b>encapsulation dot1q (service instance)</b>	Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance.
	<b>service instance (interface)</b>	Configures an Ethernet service instance on an interface and enters service instance configuration mode.

# ethernet subscriber session

To specify the minimum and maximum dynamic Ethernet sessions that can be created under an Ethernet Layer 2 (L2) context, use the **ethernet subscriber session** command. To disable this command, use the no form of this command.

**ethernet subscriber session** {**maximum** | **watermark**} **limit** *session-limit*  
**no ethernet subscriber session**

## Syntax Description

<b>maximum</b>	Specifies the maximum Ethernet sessions that can be created under an Ethernet L2 context.
<b>watermark</b>	Specifies the lower watermark. That is, the threshold limit of Ethernet sessions that can be created under an Ethernet L2 context.
<b>limit</b> <i>session-limit</i>	Specifies the maximum or threshold limit for the Ethernet sessions under L2 context. Valid values are from 2 to 8000.

## Command Default

The maximum Ethernet sessions that can be created under an Ethernet L2 context depends on the platform. The watermark value will be the same as the maximum value.

## Command Modes

Service instance configuration (config-if-srv)

## Command History

Release	Modification
15.1(2)S	This command was introduced.

## Usage Guidelines

You must configure the **encapsulation dot1q** and the **ethernet subscriber** commands before specifying the maximum and threshold number for Ethernet sessions. If the threshold limit for Ethernet sessions is reached, a syslog or trap will be generated.

## Examples

The following example shows how to configure the maximum number of Ethernet sessions under L2 context:

```
Router# configure terminal
Router(config)# interface GigabitEthernet 1/25
Router(config-if)# service instance dynamic 1 ethernet
Router(config-if-srv)# encapsulation dot1q 200

Router(config-if-srv)#
 ethernet subscriber
Router(config-if-srv)#
 ethernet subscriber session maximum limit 8
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>encapsulation dot1q (service instance)</b>	Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance.
<b>ethernet subscriber</b>	Enables an Ethernet L2 context.
<b>service instance (interface)</b>	Configures an Ethernet service instance on an interface and enters service instance configuration mode.



# ethernet subscriber static

To create a static Ethernet session for configuring Ethernet Virtual Connection (EVC) accounting, use the **ethernetsubscriberstatic** command in service instance configuration mode. To disable this command, use the **no** form of this command.

**ethernet subscriber static**  
**no ethernet subscriber static**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Static Ethernet sessions are not created for the service instance.

## Command Modes

Service instance configuration (config-if-srv)

## Command History

Release	Modification
15.1(2)S	This command was introduced.

## Usage Guidelines

Before configuring the **ethernetsubscriberstatic** command, you must configure the **encapsulation** command under an Ethernet service instance. Otherwise, you cannot enable the EVC accounting for a static Ethernet session. When you disable the **encapsulation** command, the **ethernetsubscriberstatic** command configuration is also disabled.

The EVC accounting supports forwarding paths such as bridge domain, connect, and xconnect. The **ethernetsubscriberstatic** command is not mutually exclusive with forwarding paths; that is, you can configure the command before or after the forwarding paths are configured.

The xconnect and connect forwarding paths are ISG-based, and have static Ethernet sessions created when they are configured. If the xconnect or connect forwarding paths are configured before you configure the **ethernetsubscriberstatic** command, the same static Ethernet sessions are used for EVC accounting, and new sessions are not triggered. The bridge domain forwarding path does not involve ISG data path setup. Hence, although you configure the **ethernetsubscriberstatic** command after the bridge domain forwarding path is configured, new static Ethernet sessions are triggered for EVC accounting.

If the **ethernetsubscriberstatic** command is configured before any of the forwarding paths are configured, an Ethernet session is not created. When you configure the forwarding paths, the Ethernet sessions are created.

## Examples

The following example shows how to create a static session:

```
Router# configure terminal
Router(config)# interface GigabitEthernet 1/25
Router(config-if)# service instance 101 ethernet
Router(config-if-srv)# encapsulation dot1q 200

Router(config-if-srv)# ethernet subscriber static
Router(config-if-srv)# bridge-domain 100
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>encapsulation dot1q (service instance)</b>	Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance.
<b>bridge-domain (service instance)</b>	Binds a service instance or a MAC tunnel to a bridge domain instance.
<b>service instance (interface)</b>	Configures an Ethernet service instance on an interface and enters service instance configuration mode.

# ethernet tcn-propagation

To enable topology change notification (TCN) propagation from a source protocol to a destination protocol, use the **ethernet tcn-propagation** command in global configuration mode. To disable TCN propagation, use the **no** form of this command.

```
ethernet tcn-propagation G8032 to {REP | G8032}
no ethernet tcn-propagation G8032 to {REP | G8032}
```

Syntax Description	Parameter	Description
	<b>G8032</b>	Specifies the G.8032 Ethernet Ring Protocol (ERP).
	<b>to</b>	Indicates TCN propagation from the source protocol to the destination protocol.
	<b>REP</b>	Specifies the Resilient Ethernet Protocol (REP).

**Command Default** TCN propagation is disabled.

**Command Modes** Global configuration (config)

Command History	Release	Modification
	Cisco IOS XE Release 3.6S	This command was introduced.
	15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
	15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

**Usage Guidelines** The G.8032 and REP protocols are the source and destination protocols available, although the protocols can vary by platform and release.

The G.8032 and REP protocols can be used in the following source-to-destination combinations:

- G.8032 to REP
- G.8032 to G.8032

## Examples

The following is an example of the **ethernet tcn-propagation** command used in an Ethernet ring configuration.

```
Device> enable
Device# configure terminal
Device(config)# ethernet tcn-propagation G8032 to G8032
```

# ethernet uni

To set user-network interface (UNI) bundling attributes, use the **ethernet uni** command in interface configuration mode. To return to the default bundling configuration, use the **no** form of this command.

```
ethernet uni [{bundle [all-to-one] | id uni-id | multiplex}]
no ethernet uni
```

## Syntax Description

<b>bundle</b>	(Optional) Configures the UNI to support bundling without multiplexing.
<b>all-to-one</b>	(Optional) Configures the UNI to support bundling with a single Ethernet virtual connection (EVC) at the UNI and all CE VLANs mapped to that EVC.
<b>id</b>	(Optional) Configures a UNI ID.
<i>uni-id</i>	(Optional) String of 1 to 64 alphanumeric characters that identifies the UNI. The name should be unique for all UNIs that are part of a given service instance.
<b>multiplex</b>	(Optional) Configures the UNI to support multiplexing without bundling.

## Command Default

If bundling or multiplexing attributes are not configured, the default is bundling with multiplexing. The UNI then has one or more EVCs with one or more CE VLANs mapped to each EVC.

## Command Modes

Interface configuration (config-if)

## Command History

Release	Modification
12.2(25)SEG	This command was introduced.
12.2(33)SRB	This command was implemented on the Cisco 7600 series routers.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

## Usage Guidelines

UNI options determine the functionality that the interface has regarding bundling VLANs and multiplexing EVCs.

If you want only the bundling or only the multiplexing service, you must configure the service appropriately. Bundling supports only one EVC at the UNI with one or multiple customer edge (CE)-VLAN IDs mapped to the EVC.

When multiplexing is configured, the UNI can have one or more EVCs with a single CE-VLAN ID mapped to each EVC.

When you configure a UNI ID on a port, that ID is used as the default name for all maintenance end points (MEPs) configured on the port.

You must enter the **ethernet uni** command with the **id** keyword and *id* argument on all ports that are directly connected to CE devices. When the specified ID is not unique on a device, an error message is displayed.

When you configure, change, or remove a UNI service type, the EVC and CE-VLAN ID configurations are checked to ensure that the configurations and the UNI service types match. If the configurations do not match, the command is rejected.

## Examples

The following example shows how to configure bundling without multiplexing:

```
Device(config)# interface ethernet 2/1
Device(config-if)# ethernet uni bundle
```

This example shows how to identify a UNI as test2:

```
Device(config)# interface ethernet 2/1
Device(config-if)# ethernet uni id test2
```

## Related Commands

Command	Description
<b>show ethernet service interface</b>	Displays information about Ethernet service instances on an interface, including service type.

## event ethernet microwave clear-sd

To create an Ethernet microwave event to be associated with bandwidth signal degradation (SD) occurrences, use the **event ethernet microwave clear-sd** command in applet configuration mode. To delete the Ethernet microwave event, use the **no** form of this command.

**event ethernet microwave clear-sd interface** *type number*

**no event ethernet microwave clear-sd**

### Syntax Description

<b>interface</b> <i>type number</i>	Specifies the type and number of the interface.
-------------------------------------	---

### Command Default

The SD indicator is not cleared.

### Command Modes

Applet configuration (config-applet)

### Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

### Usage Guidelines

Use the **event manager applet** command to enter applet configuration mode.

The **event ethernet microwave clear-sd** command creates the Ethernet microwave event to be associated with bandwidth signal degradation (SD) occurrences. After creating the event, use the **action switch ring g8032 clear instance** to clear the SD occurrence and bring the ring back to the normal (idle) state.

### Examples

The following is an example of the **event ethernet microwave clear-sd** command configured as part of an Ethernet microwave event. In this configuration, GigabitEthernet interface 0/1/0 is specified:

```
Device> enable
Device# configure terminal
Device(config)# event manager applet mw_ring_sd1
Device(config-applet)# event ethernet microwave clear-sd interface gigabitethernet 0/1/0
Device(config-applet)# action 2 switch ring g8032 clear instance all
Device(config-applet)#
```

### Related Commands

Command	Description
<b>action switch ring g8032 clear instance</b>	Specifies the action of clearing a SD occurrence on a link of a G.8032 ERP topology.
<b>event manager applet</b>	Registers an applet with the EEM and enters applet configuration mode.

## event ethernet microwave sd

To create the Ethernet microwave signal degradation (SD) event for a given interface, use the **event ethernet microwave sd** command in applet configuration mode. To delete the event, use the **no** form of this command.

```
event ethernet microwave sd {interface type number
[mac-addressmac-address | link-idlink-id] threshold threshold-bandwidth}
```

```
no event ethernet microwave sd
```

### Syntax Description

<b>interface</b> <i>type number</i>	Specifies the type and number of the interface.
<b>threshold</b> <i>threshold-bandwidth</i>	Specifies the threshold bandwidth, in MB/s. Enter a number from 0 to 2147483647.
<b>mac-address</b> <i>mac-address</i>	(Optional) Specifies the source MAC address.
<b>link-id</b> <i>link-id</i>	(Optional) Specifies the link ID of the event

### Command Default

The SD event for a given interface is not created.

### Command Modes

Applet configuration (config-applet)

### Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.
Cisco IOS XE Release 3.16S	The mac-address and link-id parameters are introduced on the Cisco ASR 900 Series Routers to support registration of individual links identified either by source MAC address or link ID.

### Usage Guidelines

Use the **event manager applet** command to enter applet configuration mode.

After the event is defined, use the **action switch ring g8032 instance** command to specify the appropriate action to take on this event.

### Examples

The following is an example of the **event ethernet microwave sd** command configured as part of an Ethernet microwave event:

```
Device> enable
Device# configure terminal
Device(config)# event manager applet mw_ring_sd1
Device(config-applet)# event ethernet microwave sd interface gigabitethernet 0/1/0 threshold
30
```

```
Device(config-applet)# action 1 switch ring g8032 ringA instance 1
Device(config-applet)#
```

**Related Commands**

Command	Description
<b>action switch ring instance</b>	Specifies the protocol switch action for an instance on a link of a G.8032 ERP topology.
<b>event manager applet</b>	Registers an applet with the EEM and enters applet configuration mode.



## exclusion-list

To define a set of VLAN IDs that the Ethernet ring protection mechanism does not protect, use the **exclusion-list** command in Ethernet ring configuration mode. To delete the set of VLAN IDs that are unprotected, use the **no** form of this command.

```
exclusion-list vlan-ids vlan-id [,vlan-range][,vlan-range][,vlan-range]  
no exclusion-list vlan-ids
```

Syntax Description	vlan-ids	Associates a set of VLAN IDs with the current instance.
	<i>vlan-id</i>	A single VLAN from 1 to 4094.
	<i>,vlan-range</i>	(Optional) A range of VLANs from 1 to 4094 in the form of <i>n-n</i> . When specifying multiple ranges ( for example, <i>n-n</i> , <i>n-n</i> ), the , keyword must be used as a delimiter.

**Command Default** A set of unprotected VLAN IDs is not defined.

**Command Modes** Ethernet ring configuration (config-erp-ring)

Command History	Release	Modification
	Cisco IOS XE Release 3.6S	This command was introduced.
	15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
	15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

**Usage Guidelines** By default, all the VLANs configured under ring ports are blocked. The VLANs remain blocked unless they are specified by either the **exclusion-list** command or the **inclusion-list** command.

VLAN IDs specified by the **exclusion-list** command cannot also belong to the inclusion list (that is, the list of VLAN IDs that the Ethernet ring protection mechanism protects, as specified by the **inclusion-list** command). The VLAN ID ranges cannot overlap and must be unique.

### Examples

The following is an example of the **exclusion-list** command used in an Ethernet ring configuration.

```
Device> enable  
Device# configure terminal  
Device(config)# ethernet ring g8032 ring1  
Device(config-erp-ring)# exclusion-list vlan-ids 1-5, 13, 15-25
```

Related Commands	Command	Description
	<b>inclusion-list</b>	Defines a set of VLAN IDs that the Ethernet ring protection mechanism protects.

## id (CFM)

To configure a maintenance domain identifier (MDID), use the **id** command in Ethernet connectivity fault management (CFM) configuration mode. To remove a MDID, use the **no** form of this command.

```
id {mac-address domain-number | dns dns-name | null}
no id
```

### Syntax Description

<i>mac-address</i>	MAC address of the maintenance domain.
<i>domain-number</i>	Integer in the range of 0 to 65535.
<b>dns</b>	Specifies a domain name service (DNS).
<i>dns-name</i>	String of a maximum of 43 characters.
<b>null</b>	Indicates there is not a domain name.

### Command Default

A MDID is not configured.

### Command Modes

Ethernet CFM configuration (config-ecfm)

### Command History

Release	Modification
12.2(33)SX12	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

### Usage Guidelines

If the MDID is not specified, the domain name in string format is used as the default. If a DNS name exceeds 43 characters, the MDID is only the first 43 characters of that DNS name.

If the MDID is explicitly null, the maintenance association ID (MAID) is constructed from the short maintenance association name. The short maintenance association name needs to be unique globally if the MDID is null.

### Examples

The following example shows how to configure a MDID with a MAC address and a domain number:

```
Device(config)# ethernet cfm domain customerA level 5
Device(config-ecfm)# id aaaa.bbbb.cccc 1017
```

# inclusion-list

To define a set of VLAN IDs that the Ethernet ring protection mechanism protects, use the **inclusion-list** command in Ethernet ring instance configuration mode. To delete the set of VLAN IDs that are protected, use the **no inclusion-list** form of this command.

**inclusion-list** **vlan-ids** *vlan-id* [*,vlan-range*][*,vlan-range*][*,vlan-range*]  
**no inclusion-list** **vlan-ids**

Syntax Description	vlan-ids	Associates a set of VLAN IDs with the current instance.
	<i>vlan-id</i>	A single VLAN from 1 to 4094.
	<i>,vlan-range</i>	(Optional) A range of VLANs from 1 to 4094 in the form of <i>n-n</i> . When specifying multiple ranges ( for example, <i>n-n , n-n</i> ), the <i>,</i> keyword must be used as a delimiter.

**Command Default** A set of protected VLAN IDs is not defined.

**Command Modes** Ethernet ring instance configuration (config-erp-inst)

Command History	Release	Modification
	Cisco IOS XE Release 3.6S	This command was introduced.
	15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
	15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

**Usage Guidelines** Use this command when opening (resolving) a blocked Ethernet ring.

VLAN IDs specified by the **inclusion-list** command cannot also belong to the exclusion list (that is, the list of VLAN IDs that the Ethernet ring protection mechanism does not protect, as specified by the **exclusion-list** command). The VLAN ID ranges cannot overlap and must be unique.

## Examples

The following is an example of the **exclusion-list** command used in an Ethernet ring configuration.

```
Device> enable
Device# configure terminal
Device(config)# ethernet ring g8032 ring1
Device(config-erp-ring)# instance 1
Device(config-erp-inst)# inclusion-list vlan-ids 7-11, 200, 555-700
```

Related Commands	Command	Description
	<b>exclusion-list</b>	Defines a set of VLAN IDs that the Ethernet ring protection mechanism does not protect.

# ingress-replication

To set up ingress-replication unicast addresses which enables the headend replication functionality, use the **ingress-replication** command in NVE interface configuration. To delete the set of ingress-replication unicast addresses, use the **no** form of this command.

**ingress-replication** *Unicast IP Addresses*

**no ingress-replication** *Unicast IP Addresses*

<b>Syntax Description</b>	<i>Unicast IP Addresses</i> Specify one or more unicast IP addresses.
---------------------------	---

**Command Default** Ingress replication is not configured.

**Command Modes** NVE interface configuration (config-if-nve-vni)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 3.13.1S	This command was introduced.
	Cisco IOS XE Everest 16.5.1	This command was modified to support multiple ingress replication peers.

**Usage Guidelines** To use this command create a VNI member or a range of VNI members to which the ingress-replication peers are associated.

## Examples

The following is an example of the **ingress-replication** command used in an NVE interface configuration.

```
Router(config)# interface nve 1
Router(config-if)# source-interface loopback 0
Router(config-if)# member vni 7115
Router(config-if-nve-vni)# ingress-replication 198.51.100.1
Router(config-if-nve-vni)# ingress-replication 198.51.100.2
```

## initiator unclassified vlan

To enable an initiator for detecting the first sign of life (FSoL) under an Ethernet Layer 2 context, use the **initiator** command in service instance configuration mode. To disable the initiator, use the **no** form of the command.

### initiator unclassified vlan

#### Syntax Description

This command has no arguments or keywords.

#### Command Default

The initiator is not enabled under the Ethernet Layer 2 context.

#### Command Modes

Service instance configuration (config-if-srv)

#### Command History

Release	Modification
15.1(2)S	This command was introduced.

#### Usage Guidelines

Ethernet Layer 2 context defines the control plane policy for detecting FSoL. When you configure the **initiator** command under the Ethernet Layer 2 context, FSoLs are attracted based on the FSoL mechanism specified and dynamic Ethernet sessions are created. Cisco IOS Release 15.1(2)S supports the unclassified VLAN FSoL mechanism.

An unclassified VLAN frame that is classified in a Layer 2 context service instance is sent to the route processor (RP) to create an Ethernet Layer 2 session.

#### Examples

The following example shows how to enable the initiator under an Ethernet Layer 2 context to attract FSoL:

```
Router# configure terminal
Router(config)# interface Ethernet 0/0
Router(config-if)# service instance dynamic 2 ethernet
Router(config-if-
srv)# encapsulation dot1q 200
```

```
Router(config-if-srv)# ethernet subscriber
Router(config-if-srv)# initiator unclassified vlan
```

#### Related Commands

Command	Description
<b>encapsulation dot1q (service instance)</b>	Defines the matching criteria to map 802.1Q frames received on an interface to the appropriate service instance.
<b>ethernet subscriber</b>	Enables an Ethernet Layer 2 context.
<b>service instance (interface)</b>	Configures an Ethernet service instance on an interface and enters service instance configuration mode.

# input

To enable Precision Time Protocol input clocking using a 1.544Mhz, 2.048Mhz, or 10Mhz timing interface or phase using the 1PPS or RS-422 interface, use the **input** command in global configuration mode. To disable PTP input, use the **no** form of this command.

**input** [**1pps**] *slot/bay*  
**no input** [**1pps**] *slot/bay*

## Syntax Description

<b>1pps</b>	Configures the device to receive 1 pulse per second (1PPS) time of day messages using the RS422 port or 1PPS port. You can select 1PPS with or without selecting a timing port.
<i>slot</i>	Slot of the 1PPS interface.
<i>bay</i>	Bay of the 1PPS interface.

## Command Default

Precision Time Protocol input clocking is not enabled.

## Command Modes

Global configuration (config)

## Command History

Release	Modification
12.2(31)SB2	This command was introduced.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

## Usage Guidelines

If you are using GPS to provide clock source to the device, configure this command in PTP master mode. This command applies only to platforms that have a 1PPS port.

## Examples

The following example shows how to configure PTP input clocking:

```
Device> enable
Device# configure terminal
Device(config)# ptp clock ordinary domain 0
Device(config-ptp-clk)# input 1pps 3/1
Device(config-ptp-clk)# clock-port masterport master
```

## Related Commands

Command	Description
<b>output</b>	Enables output of time of day messages using the 1PPS interface.

## l2 subscriber

To create a Layer 2 (L2) subscriber authorization group and enter L2 subscriber group mode, use the **l2subscriber** command in global configuration mode. To remove the L2 subscriber authorization group, use the **no** form of this command.

```
l2 subscriber authorization group group-name
no l2 subscriber authorization group group-name
```

Syntax Description	Command	Description
	<b>authorization group</b>	Creates an L2 subscriber authorization group.
	<i>group-name</i>	Name of the L2 subscriber authorization group.

**Command Default** L2 subscriber authorization group is not created.

**Command Modes** Global configuration (config)

Command History	Release	Modification
	15.1(2)S	This command was introduced.

**Usage Guidelines** You can use the **l2subscriber** command to create a named service authorization group and enter into L2 subscriber group mode.

You can define multiple L2 subscriber authorization groups on the router. Each group essentially defines a set of Any Transport over MPLS (AToM) peers using the peer's Multiprotocol Label Switching (MPLS) label distribution protocol (LDP) router ID (IP address or IP address network) and virtual circuit (VC) ID or range. You must be sure to define mutually exclusive service authorization groups.

You can use configuration commands available in L2 subscriber group mode to enable an AToM or label advertisement to be used for First Sign of Life (FSOL) processing.

When an AToM LDP label advertisement is received and there is a matching group, the ISG control policy-map is executed and the AAA attributes for the corresponding xconnect is downloaded from RADIUS. Thus, a dynamic xconnect will be provisioned for the peer provider edge (PE). You can use the **showderived-configinterface** command to see the details of the xconnect that is downloaded.

To provide a description for the L2 subscriber authorization group, use the **description** command in L2 subscriber group mode.

### Examples

The following example shows how to create an L2 subscriber authorization group:

```
Router# configure terminal
Router(config)# l2 subscriber authorization group group1
```

Related Commands	Command	Description
	<b>peer</b>	Defines the target LDP PE peer information.

Command	Description
<b>pseudowire (Layer 2)</b>	Defines the maximum and watermark limits for pseudowires from a peer PE device.
<b>service-policy type control (Layer 2)</b>	Attaches an ISG control service policy to an L2 subscriber authorization group.



# lACP active-port distribution automatic

To have an effective auto interleaved port priority distribution of active and bundled ports across different slots that are part of the same port channel distributed EtherChannel (DEC) and multichassis EtherChannel (MEC), use the **lACP active-port distribution automatic** command in port channel configuration mode.

**lACP active-port distribution automatic**  
**no lACP active-port distribution automatic**

**Syntax Description** This command has no keywords or arguments.

**Command Default** Auto interleaved port priority is disabled.

**Command Modes** Interface configuration (config-if)

Command History	Release	Modification
	12.2(33)SX14	This command was introduced.

**Usage Guidelines** The auto interleaved port-priority feature automatically distributes active and bundled ports based on the position of a port link when it comes up and is effective only if you configure it on the system that has the higher LACP system priority.

The port priority per port that you configured continues to take precedence over a dynamic port number. You need to perform a shutdown and no shutdown on the interface port channel to enable the auto interleaved port priority feature on all ports.

## Examples

This example shows how to configure interleaved port priority:

```
Router(config)# interface port23
Router(config-if)# lACP active-port distribution automatic
Please shut/no shut the port-channel for configuration to take effect immediately.
Router(config-if)# shutdown
Router(config-if)# no shutdown
Router(config-if)# end
```

This example shows how to verify that interleaved port priority is configured:

```
Router# show running interface port23
Building configuration...
Current configuration : 81 bytes
!
interface Port-channel23
no switchport
no ip address
lACP max-bundle 4
lACP active-port distribution automatic
end
Router# show etherchannel 23 summary
Flags: D - down P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
```

```

U - in use N - not in use, no aggregation
f - failed to allocate aggregator
M - not in use, no aggregation due to minimum links not met
m - not in use, port not aggregated due to minimum links not met
u - unsuitable for bundling
d - default port
w - waiting to be aggregated
Number of channel-groups in use: 9
Number of aggregators: 9
Group      Port-channel Protocol      Ports
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
23         Po23 (RU)          LACP          Gi1/1/21 (P) Gi1/1/22 (P) Gi1/1/23 (P)
                                     Gi1/1/24 (P) Gi2/1/17 (H) Gi2/1/18 (H)
                                     Gi2/1/19 (H) Gi2/1/20 (H)

Last applied Hash Distribution Algorithm: Fixed

```




---

**Note** The four active and bundled ports are from the same chassis and slot.

---

#### Related Commands

Command	Description
<b>show etherchannel</b>	Displays EtherChannel information for a port channel.

# lACP direct-loadswap

To enable Link Aggregation Control Protocol (LACP) direct load swapping on a port channel, use the **lACP direct-loadswap** command in interface port-channel configuration mode. To return to the default setting, use the **no** form of this command.

**lACP direct-loadswap**  
**no lACP direct-loadswap**

**Syntax Description** This command has no arguments or keywords.

**Command Default** Direct loadswapping is disabled.

**Command Modes** Interface port-channel configuration (config-if)

Command History	Release	Modification
	12.2(33)SRC	This command was introduced.

**Usage Guidelines** Use this command to enable the LACP Single Fault Direct Load Balance Swapping feature on a port channel. This command can be used for only a single bundled port failure. If a second failure occurs before the first failure recovers, the loadshare bits for member links are recomputed.

## Examples

This example shows how to enable LACP single fault direct load swapping on port channel 1:

```
Router(config)# interface port-channel 1
Router(config-if)# lACP direct-loadswap
Router(config-if)#
```

## Related Commands

Command	Description
<b>interface port-channel</b>	Creates a port-channel virtual interface and places the CLI in interface configuration mode.
<b>show etherchannel</b>	Displays the EtherChannel information for a channel.
<b>show interfaces port-channel</b>	Displays traffic that is seen by a specific port channel.

# lACP failover

To set the Multichassis Link Aggregation Control Protocol (mLACP) failover mechanism to bring down a active physical member link interface(s) for a given link aggregation group (LAG) on the point of attachment (PoA) that is surrendering its active status, use the **lACP failover** command in port-channel interface configuration mode. To return to the default setting, use the **no** form of this command.

**lACP failover** {brute-force | non-revertive}  
**no lACP failover**

## Syntax Description

<b>brute-force</b>	Brute-force failover places the PoA links in the ERR_DISABLE state.
<b>non-revertive</b>	Non-revertive mode is used to limit failover and possible traffic loss when a failed PoA recovers by not reverting to the Active role.

## Command Default

The command is in revertive mode (with 180-second delay) and uses the dynamic port priority failover mechanism.

## Command Modes

Port-channel interface configuration (config-if)

## Command History

Release	Modification
12.2(33)SRE	This command was introduced.

## Usage Guidelines

The default dynamic port priority failover mechanism provides the best failover performance.

A brute-force shutdown doesn't depend on the dual-homed device's (DHD's) ability to handle dynamic port priority changes and compensates for deficiencies in the DHD's LACP implementation.

The brute-force and non-revertive modes are mutually exclusive.

The brute-force shutdown changes the status of each member link to ERR\_DISABLE to force the transition of the standby links to active state. This process eliminates the ability of the local LACP implementation to monitor the link state.

A brute force shutdown operates in revertive mode-- dynamic port priorities cannot be used to control active selection.

Dynamic port priority failover is used by the mLACP feature in both revertive mode and non-revertive mode.

Non-revertive mode is used to limit failover and therefore, possible traffic loss. Dynamic port priority changes are used to ensure that the newly activated point of attachment (PoA) remains active after the failed PoA recovers.

Revertive mode operation forces the primary PoA to return to active state after it recovers from a failure. Dynamic port priority changes are used when necessary to allow the recovering PoA to resume its active role.

## Examples

This example shows how to set the LACP failover for non-revertive mode:

```
interface Port-channel1
  lACP max-bundle 3
  lACP min-bundle 2
```

```
lacp failover non-revertive
mlacp lag-priority 1000
mlacp interchassis group 1
service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100 c-mac
```

**Related Commands**

Command	Description
<b>errdisable recovery cause mlacp-minlink</b>	Enables automatic recovery from a failover state of the port channel and specifies the interval for recovery.
<b>interface port-channel</b>	Creates a port-channel virtual interface and puts the CLI in interface configuration mode.

# lACP fast-switchover

To enable Link Aggregation Control Protocol (LACP) 1:1 link redundancy, use the **lACP fast-switchover** command in interface configuration mode. To disable LACP 1:1 link redundancy, use the **no** form of this command.

**lACP fast-switchover**  
**no lACP fast-switchover**

**Syntax Description** This command has no arguments or keywords.

**Command Default** LACP 1:1 link redundancy is disabled by default.

**Command Modes** Interface configuration (config-if)

## Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	Support for this command was implemented on the Cisco 10000 series router and integrated into Cisco IOS Release 12.2(33)SB. The time allowed for a link switchover was modified from the default of 2 seconds to 250 milliseconds.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5

## Usage Guidelines

Prior to entering the **lACP fast-switchover** command, you must ensure the following:

- The port channel protocol type is LACP.
- The **lACP max-bundle 1** command has been entered on the port channel. The **lACP fast-switchover** command will not affect the **lACP max-bundle** command.

When you enable LACP 1:1 link redundancy, based on the system priority and port priority, the port with the higher system priority chooses the link as the active link and the other link as the standby link. When the active link fails, the standby link is selected as the new active link without taking down the port channel. When the original active link recovers, it reverts to its active link status. During this change-over, the port channel is also up.



**Note** We recommend that you configure two ports only (one active and one hot-standby) in the bundle for optimum performance.

You can enter this command on any port channels with different EtherChannel protocol types of LACP, Port Aggregation Protocol (PAgP), or Fast EtherChannel (FEC).

## Examples

This example shows how to enable LACP 1:1 link redundancy:

```
Router(config-if)# lacp fast-switchover
```

This example shows how to disable LACP 1:1 link redundancy:

```
Router(config-if)# no lacp fast-switchover
```

**Related Commands**

Command	Description
<b>lacp max-bundle</b>	Assigns and configures an EtherChannel interface to an EtherChannel group.
<b>show etherchannel</b>	Displays the EtherChannel information for a channel.

# lACP max-bundle

To define the maximum number of active bundled Link Aggregation Control Protocol (LACP) ports allowed in a port channel, use the **lACP max-bundle** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

**lACP max-bundle** *max-bundles*  
**no lACP max-bundle**

## Syntax Description

<i>max-bundles</i>	<p>Maximum number of active bundled ports allowed in the port channel. Valid values are from 1 to 8. On the Cisco ASR 1000 series router, valid values are 1 to 4.</p> <p>The default settings are as follows:</p> <ul style="list-style-type: none"> <li>• Maximum of 8 bundled ports per port channel.</li> <li>• Maximum of 8 bundled ports and 8 hot-standby ports per port channel if the port channels on both sides of the LACP bundle are configured in the same way.</li> <li>• On the Cisco 10000 series router, maximum of 8 bundled ports per port channel.</li> </ul>
--------------------	--

## Command Default

A maximum number of active bundled ports is not configured.

## Command Modes

Interface configuration (config-if)

## Command History

Release	Modification
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	Support for this command was implemented on the Cisco 10000 series router and integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	Support for this command on the Cisco 7600 router was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	On the Cisco 10000 series router, the maximum number of bundled ports per port channel was increased from 4 to 8.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

## Usage Guidelines

The value specified in the *max-bundles* argument determines the number of active links that are bundled in the port channel. The remaining links are in hot-standby mode.

On the Cisco 10000 series router, this command requires a Performance Routing Engine 2 (PRE2) or PRE3.

## Examples

This example shows how to set 3 ports to bundle in port channel 2:



```
Router(config)# interface port-channel 2
Router(config-if)# lacp max-bundle 3
Router(config-if)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>interface port-channel</b>	Creates a port-channel virtual interface and puts the CLI in interface configuration mode.
<b>ip address</b>	Sets a primary or secondary IP address on an interface.
<b>show etherchannel</b>	Displays the EtherChannel information for a channel.
<b>show interfaces port-channel</b>	Displays traffic that is seen by a specific port channel.

# lACP min-bundle

To set the minimum number of active links in a Link Aggregation Control Protocol (LACP) bundle, use the **lACP min-bundle** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

**lACP min-bundle** *min-bundle*  
**no lACP min-bundle**

## Syntax Description

<i>min-bundle</i>	Minimum number of bundled ports allowed in the port channel. Valid values are from 1 to 8. The default is 1.
-------------------	--

## Command Default

The port-channel operational state will be “Down” only when there are no active links in the channel. If there are one or more active links, the port-channel state will be “Up.”

## Command Modes

Interface configuration (config-if)

## Command History

Release	Modification
12.2(33)SB	This command was introduced.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

## Usage Guidelines

Use the **lACP min-bundle** command to configure the minimum number of active links allowed in an LACP bundle. When the number of active links falls below this minimum threshold, the port channel shuts down.



**Note** LACP and the same minimum bundle value must be configured on each peer in order for both sides of the port channel to be brought down.

### Cisco 10000 Series Router

This command requires a Performance Routing Engine 2 (PRE2) or PRE3.

## Examples

This example shows how to set the minimum number of active links to 5 ports:

```
Device(config-if)# lACP min-bundle 5
```

## Related Commands

Command	Description
<b>interface port-channel</b>	Creates a port-channel virtual interface and enters interface configuration mode.
<b>ip address</b>	Sets a primary or secondary IP address on an interface.
<b>show etherchannel</b>	Displays the EtherChannel information for a channel.

Command	Description
<b>show interfaces port-channel</b>	Displays traffic that is seen by a specific port channel.

# lACP port-priority

To set the priority for a physical interface, use the **lACP port-priority** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

**lACP port-priority** *priority*

**no lACP port-priority**

## Syntax Description

<i>priority</i>	Integer from 1 to 65535 that indicates the priority for the physical interface. The default is 32768. <ul style="list-style-type: none"> <li>On the Cisco ASR 1000 series router, the range is 0 to 65535.</li> </ul>
-----------------	--

## Command Default

The default port priority is set.

## Command Modes

Interface configuration (config-if)

## Command History

Release	Modification
12.1(13)EW	This command was introduced on the Cisco Catalyst 4500 series switches.
12.2(14)SX	Support for this command on the Supervisor Engine 720 was integrated into Cisco IOS Release 12.2(14)SX.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was integrated into Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	Support for this command on the Cisco 7600 router was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

## Usage Guidelines

You may assign a port priority to each port on a device running Link Aggregation Control Protocol (LACP). You can specify the port priority by using the **lACP port-priority** command at the command-line interface (CLI) or use the default port priority (32768) that is carried as part of the LACP protocol data unit (PDU) exchanged with the partner. Port priority is used to decide which ports should be put in standby mode when a hardware limitation or the **lACP max-bundle** command configuration prevents all compatible ports from aggregating. Priority is supported only on port channels with LACP-enabled physical interfaces.



**Note** A high priority number means a low priority.

Port priority together with port number form a port identifier.

To verify the configured port priority, issue the **show lACP** command.

### Examples

This example shows how to set a priority of 23700 for an interface:

```
Device> enable
Device# configure terminal
Device(config)# interface ethernet0/0
Device(config-if)# lACP port-priority 23700
Device(config-if)#
```

### Related Commands

Command	Description
<b>channel-group</b>	Assigns and configures an EtherChannel interface to an EtherChannel group.
<b>debug lACP</b>	Enables debugging of LACP activities.
<b>lACP max-bundle</b>	Defines the maximum number of active bundled LACP ports allowed in a port channel.
<b>lACP system-priority</b>	Sets the priority of the system.
<b>show lACP</b>	Displays information about LACP activity on the device.

# lACP rate

To set the rate at which Link Aggregation Control Protocol (LACP) control packets are ingressed to an LACP-supported interface, use the **lACP rate** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

**lACP rate** {normal | fast}  
**no lACP rate**

## Syntax Description

<b>normal</b>	Specifies that LACP control packets are ingressed at the normal rate, every 30 seconds after the link is bundled.
<b>fast</b>	Specifies that LACP control packets are ingressed at the fast rate, once every 1 second.

## Command Default

The default ingressed rate for control packets is 30 seconds after the link is bundled.

## Command Modes

Interface configuration (config-if)

## Command History

Release	Modification
12.2(18)SXF2	This command was introduced on the Catalyst 6500 series switch.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 3.6S	This command was implemented on Cisco ASR 1000 Series Aggregation Services Routers in Cisco IOS XE Release 3.6S.

## Usage Guidelines

Use this command to modify the duration of a LACP timeout. The LACP timeout value is set on Cisco switches to a value of 90 seconds. Using the **lACP rate** command, you can select the LACP timeout value for a switch to be either 30 seconds or 1 second.

This command is supported only on LACP-enabled interfaces.

## Examples

This example shows how to specify the fast (1-second) ingress rate on interface Ethernet 0/1:

```
Router(config)# interface ethernet 0/1
Router(config-if)# lACP rate fast
```

## Related Commands

Command	Description
<b>show lACP</b>	Displays LACP information.

# lACP system-priority

To set the priority for a system, use the **lACP system-priority** command in global configuration mode. To return to the default setting, use the **no** form of this command.

**lACP system-priority** *priority*

**no lACP system-priority**

<b>Syntax Description</b>	<p><i>priority</i> Integer from 1 to 65535 that indicates the priority for the system. The default is 32768.</p> <ul style="list-style-type: none"> <li>On the Cisco ASR 1000 series router, the range is 0 to 65535.</li> </ul>
---------------------------	--

**Command Default** The default system priority is set.

**Command Modes** Global configuration (config)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(13)EW	This command was introduced on the Cisco Catalyst 4500 series switches.
	12.2(14)SX	Support for this command on the Supervisor Engine 720 was integrated into Cisco IOS Release 12.2(14)SX.
	12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was integrated into Cisco IOS Release 12.2(17d)SXB.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
	12.2(33)SRB	Support for this command on the Cisco 7600 router was integrated into Cisco IOS Release 12.2(33)SRB.
	Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4.
	15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

**Usage Guidelines** You can assign a system priority to each device running Link Aggregation Control Protocol (LACP). You can specify the system priority by using the **lACP system-priority** command at the command-line interface (CLI) or use the default system priority (32768) that is carried as part of the LACP protocol data unit (PDU) exchanged with the partner. System priority is used with the MAC address of the device to form the system ID and also is used during negotiation with other systems. Priority is supported only on port channels with LACP-enabled physical interfaces.



**Note** A high priority number means a low priority.

To verify the configured system priority, issue the **show lacp** command.

### Examples

The following example shows how to set a system priority of 25500 for a device:

```
Router> enable
Router# configure terminal
Router(config)# lacp system-priority 25500
```

### Related Commands

Command	Description
<b>channel-group</b>	Assigns and configures an EtherChannel interface to an EtherChannel group.
<b>debug lacp</b>	Enables debugging of LACP activities.
<b>lacp port-priority</b>	Sets the priority of a port.
<b>show lacp</b>	Displays information about LACP activity on the device.



## level (CFM-AIS-link)

To configure a maintenance level to receive Alarm Indication Signal (AIS) frames transmitted by a link-status change (server maintenance endpoint [SMEP]), use the **level** command in CFM SMEP AIS configuration mode. To remove the maintenance level, use the **no** form of this command.

**level** *level-id*  
**no level**

<b>Syntax Description</b>	<i>level-id</i> Integer from 0 to 7 that specifies the maintenance level.
---------------------------	---

**Command Default** A maintenance level is not configured.

**Command Modes** CFM SMEP AIS configuration (config-ais-link-cfm)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(33)SRD	This command was introduced.
	15.0(1)XA	This command was integrated into Cisco IOS Release 15.0(1)XA.
	15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
	Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

**Usage Guidelines** This command allows you to transmit AIS messages to a higher level maintenance association without configuring a maintenance intermediate point (MIP) for the service.

### Examples

The following example shows how to configure maintenance level 5 as the level to receive AIS frames transmitted by a link-status change:

```
Device(config)# ethernet cfm ais link-status global
Device(config-ais-link-cfm)# level 5
```

# level

To set the Automatic Protection Switching (APS) message level, use the **level** command in Ethernet ring instance aps-channel configuration mode. To delete the APS message level setting, use the **no** form of this command.

**level** *level-value*

**no level**

## Syntax Description

<i>level-value</i>	Enter a number from 0 to 7.
--------------------	-----------------------------

## Command Default

The default APS message level is 7.

## Command Modes

Ethernet ring instance aps-channel configuration (config-erp-inst-aps)

## Command History

Release	Modification
Cisco IOS XE Release 3.6S	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

## Usage Guidelines

This command specifies the APS message level for the node on the Ethernet ring. All nodes in the Ethernet ring must be set at the same level.

## Examples

The following is an example of the **level** command used in an Ethernet ring configuration.

```
Device> enable
Device# configure terminal
Device(config)# ethernet ring g8032 ring1
Device(config-erp-ring)# instance 1
Device(config-erp-inst)# aps-channel
Device(config-erp-inst-aps)# level 4
```

# lldp

To enable and configure Link Layer Discovery Protocol (LLDP), use the **lldp** command in global configuration mode. To disable LLDP, use the **no** form of this command.

```
lldp {holdtime seconds | reinit delay | run | timer rate | tlv-select tlv}
no lldp {holdtime | reinit | run | timer | tlv-select tlv}
```

## Syntax Description

<b>holdtime</b>	Specifies the length of time that the receiver must keep the packet.
<i>seconds</i>	Integer in the range from 0 to 65535 that specifies the length of time, in seconds, that the receiver must keep the packet. The default is 120.
<b>reinit</b>	Specifies a delay for LLDP initialization on an interface.
<i>delay</i>	Integer in the range from 2 to 5 that specifies the length of time, in seconds, that LLDP should wait to initialize. The default is 2.
<b>run</b>	Enables LLDP.
<b>timer</b>	Specifies a rate at which LLDP packets are sent.
<i>rate</i>	Integer in the range from 5 to 65534 that specifies how often, in seconds, the Cisco IOS software sends LLDP updates. The default is 30.
<b>tlv-select</b>	Specifies the time-length-value (TLV) elements to send.
<i>tlv</i>	String that identifies the TLV element to use. Valid values are: <ul style="list-style-type: none"> <li>• <b>mac-phy-cfg</b> --IEEE 802.3 MAC/Phy configuration/status TLV</li> <li>• <b>management-address</b> --Management address TLV</li> <li>• <b>port-description</b> --Port description TLV</li> <li>• <b>port-vlan</b> --Port VLAN ID TLV</li> <li>• <b>system-capabilities</b> --System capabilities TLV</li> <li>• <b>system-description</b> --System description TLV</li> <li>• <b>system-name</b> --System name TLV</li> </ul>

## Command Default

LLDP is globally disabled. No LLDP advertisements are sent.

## Command Modes

Global configuration (config)

## Command History

Release	Modification
12.2(37)SE	This command was introduced.
12.2(44)SE	This command was modified. The command default was changed to disabled.

Release	Modification
12.2(44)SG	This command was integrated into Cisco IOS Release 12.2(44)SG.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS Release XE3.8S

### Usage Guidelines

To enable LLDP, use this command with the **run** keyword.

LLDP packets are sent with a hold-time value. The receiving device ages the LLDP information about the neighbor after the hold time has elapsed.

LLDP is an industry standard version for Cisco Discovery Protocol (CDP). Non-Cisco phones use LLDP to configure voice VLANs. If you install a non-Cisco phone that supports LLDP and do not want to configure a voice VLAN on the phone, then you can use LLDP.

### Examples

The following example shows how to configure a hold time of 100 seconds:

```
Device(config)# lldp holdtime 100
```

The following example shows how to set the timer to send LLDP updates every 75 seconds:

```
Device(config)# lldp timer 75
```

### Related Commands

Command	Description
<b>show lldp</b>	Displays global LLDP information.

# lldp enable

To enable Link Layer Discovery Protocol (LLDP) in service instance, use the **lldp enable** command in service instance configuration mode. To disable LLDP, use the **no** form of this command.



**Note** Do not use the **lldp enable** command on untagged service instances.

**lldp enable**  
**no lldp enable**

**Command Default** LLDP is globally disabled.

**Command Modes** Service instance configuration (config-if-srv)

Command History	Release	Modification
	17.10.1	This command was introduced.

**Usage Guidelines** Use the **lldp enable** command per service instance, and whenever there's a need to run LLDP frames traffic over a service instance. The packets are exchanged and processed based on the encapsulation type of the service instance.

LLDP packet transmission is supported with tagged packets over a service instance with dot1q encapsulation.

## Examples

The following example shows, how to enable LLDP in a service instance on tagged packets.

```
Router#configure terminal
Router(config)#lldp run
Router(config)#interface TenGigabitEthernet0/2/0
Router(config-if)#service instance 20 ethernet
Router(config-if-srv)#encapsulation dot1q 20
Router(config-if-srv)#l2protocol peer lldp
Router(config-if-srv)#lldp enable
Router(config-if-srv)#bridge-domain 20
Router(config-if-srv)#exit
```

Related Commands	Command	Description
	<b>show lldp</b>	Displays global LLDP information.

## lldp (interface)

To enable Link Layer Discovery Protocol (LLDP) on an interface, use the **lldp** command in interface configuration mode. To disable LLDP on an interface, use the **no** form of this command.

**lldp** {**med-tlv-select** *tlv* | **receive** | **transmit**}  
**no lldp** {**med-tlv-select** *tlv* | **receive** | **transmit**}

Syntax Description	Command	Description
	<b>med-tlv-select</b>	Selects an LLDP Media Endpoint Discovery (MED) time-length-value (TLV) element to send.
	<i>tlv</i>	String that identifies the TLV element. Valid values are the following: <ul style="list-style-type: none"> <li>• <b>inventory-management</b> --LLDP MED Inventory Management TLV</li> <li>• <b>network-policy</b> --LLDP MED Network Policy TLV</li> <li>• <b>power-management</b> --LLDP MED Power Management TLV</li> </ul>
	<b>receive</b>	Enables an interface to receive LLDP transmissions.
	<b>transmit</b>	Enables LLDP transmission on an interface.

**Command Default** LLDP is enabled on supported interfaces.

**Command Modes** Interface configuration (config-if)

Command History	Release	Modification
	12.2(33)SXH	This command was introduced.

**Usage Guidelines** This command is supported on 802.1 media types.

**Examples** The following example shows how to disable LLDP transmission on interface Ethernet 0/1:

```
Router# configure terminal
Router(config)# interface ethernet 0/1
Router(config-if)# no lldp transmit
```

The following example shows how to enable LLDP transmission on interface Ethernet 0/1:

```
Router# configure terminal
Router(config)# interface ethernet 0/1
Router(config-if)# lldp transmit
```

Related Commands	Command	Description
	<b>lldp</b>	Enables LLDP globally.

# location

To provide a description of the location of a serial device, use the **location** command in line configuration mode. To remove the description, use the **no** form of this command.

**location** *text*  
**no location**

## Syntax Description

<i>text</i>	Location description.
-------------	-----------------------

## Command Default

A location description is not provided.

## Command Modes

Line configuration (config-line)

## Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

## Usage Guidelines

The **location** command enters information about the device location and status. Use the **show users all EXEC** command to display the location information.

## Examples

In the following example, the location description for the console line is given as “Building 3, Basement”:

```
Device(config)# line console
Device(config-line)# location Building 3, Basement
```

## Related Commands

Command	Description
<b>show users</b>	Displays information about the active lines on a device.

## location (interface)

To configure location information for an interface, use the **location** command in interface configuration mode. To remove the location information for an interface, use the **no** form of this command.

**location** {**additional-location-information** *word* | **civic-location-id** *id* [**port-location**] | **elin-location-id** *id*}

**no location** {**additional-location-information** *word* | **civic-location-id** *id* [**port-location**] | **elin-location-id** *id*}

### Syntax Description

<b>additional-location-information</b>	Configures additional information for a location or place.
<i>word</i>	A word or phrase that provides additional location information.
<b>civic-location-id</b>	Configures civic location information for an interface.
<b>port-location</b>	(Optional) Specifies port-specific attributes.
<b>elin-location-id</b>	Configures emergency location identifier number (ELIN) for an interface.
<i>id</i>	The ID for the civic location or the ELIN location. The ID range is from 1 to 4095.  <b>Note</b> The identifier for the civic location in the Link-Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) TLV is limited to 250 bytes or less. To avoid error messages about available buffer space during switch configuration, be sure that the total length of all civic location information specified for each civic location ID does not exceed 250 bytes.

### Command Default

Location information for interfaces is not enabled.

### Command Modes

Interface configuration (config-if)

### Command History

Release	Modification
12.2(40)SE	This command was introduced.
12.2(55)SE	This command was modified. The <b>port-location</b> keyword was added.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

### Usage Guidelines

You can use the location command to configure location support for interfaces. When you configure the **location** command on a specific interface or on several interfaces, the location TLVs are transmitted on the respective interfaces every time CDP messages are sent. After entering the location **civic-location-id** **port-location** command, you enter civic location port configuration mode. In this mode, you can enter additional location information for every port. Use the help feature (?) for details on the additional information that you can configure in this mode. You can configure the common attributes globally and specific attributes per port. If an attribute is configured both globally and on a port, the port configuration has higher priority.



The civic location identifier must not exceed 250 bytes.

## Examples

The following example shows how to enter civic location information for an interface, and to configure additional information for civic location identifier:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# location civic-location-id 1 port-location
Device(config-if-port)# number 3560
Device(config-if-port)# building 10
```

You can verify your settings by entering the show location civic interface command.

## Related Commands

Command	Description
<b>location</b>	Configures the location information for an endpoint.
<b>show location</b>	Displays the location information for an endpoint.

## location civic-location identifier

To configure the civic location information of a device, use the **location civic-location identifier** command in global configuration mode. To remove the civic location information, use the **no** form of this command.

**location civic-location identifier** {*identifier* | **host**}  
**no location civic-location identifier** {*identifier* | **host**}

### Syntax Description

<i>identifier</i>	Name of the civic location.
<b>host</b>	Defines the host civic location.

### Command Default

The civic location information of the device is not configured.

### Command Modes

Global configuration (config)

### Command History

Release	Modification
15.1(1)SG	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

### Usage Guidelines

The **host** identifier configures the host civic location. If the identifier is not a host, the identifier only defines a civic location template that can be referenced on the interface. When you configure the **location civic-location identifier host** command or **location civic-location identifier identifier** command on a device, the command mode changes to civic location configuration mode.

The **host** keyword defines the device location. The civic location options available for configuration using the *identifier* and the **host** keyword are the same. You can specify the following civic location options in civic location configuration mode:

- **additional-code**--Sets an additional civic location code.
- **additional-location-information**--Sets additional civic location information.
- **branch-road-name**--Sets the branch road name.
- **building**--Sets building information.
- **city**--Sets the city name.
- **country**--Sets the two-letter ISO 3166 country code.
- **county**--Sets the county name.
- **default**--Sets a command to its defaults.
- **division**--Sets the city division name.
- **exit**--Exits from the civic location configuration mode.
- **floor**--Sets the floor number.

- **landmark**--Sets landmark information.
- **leading-street-dir**--Sets the leading street direction.
- **name**--Sets the resident name.
- **neighborhood**--Sets neighborhood information.
- **no**--Negates the specified civic location data and sets the default value.
- **number**--Sets the street number.
- **post-office-box**--Sets the post office box.
- **postal-code**--Sets the postal code.
- **postal-community-name**--Sets the postal community name.
- **primary-road-name**--Sets the primary road name.
- **road-section**--Sets the road section.
- **room**--Sets room information.
- **seat**--Sets seat information.
- **state**--Sets the state name.
- **street-group**--Sets the street group.
- **street-name-postmodifier**--Sets the street name postmodifier.
- **street-name-premodifier**--Sets the street name premodifier.
- **street-number-suffix**--Sets the street number suffix.
- **street-suffix**--Sets the street suffix.
- **sub-branch-road-name**--Sets the sub-branch road name.
- **trailing-street-suffix**--Sets the trailing street suffix.
- **type-of-place**--Sets the type of place.
- **unit**--Sets the unit.

You can use the **show location civic-location identifier** command to display the configured civic location details.

## Examples

The following example shows how to configure civic location information of a device:

```
Device(config)# location civic-location identifier host
Device(config-civic)# country US
Device(config-civic)# building bg113
Device(config-civic)# city Boston
Device(config-civic)# state MA
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>location custom-location identifier</b>	Configures the custom location information of a device.
<b>location geo-location identifier</b>	Configures the geographical location information of a device such as latitude, longitude, altitude, and resolution.
<b>show location civic-location identifier</b>	Displays the configured civic location details.

## location civic-location-id

To configure the port location information of a civic location ID in a device, use the **location civic-location-id** command in interface configuration mode. To remove the port location information, use the **no** form of this command.

**location civic-location-id** {*identifier* | **host** | **none**} [**port-location**]  
**no location civic-location-id** {*identifier* | **host** | **none**} [**port-location**]

Syntax Description		
	<i>identifier</i>	Name of the civic location identifier.
	<b>host</b>	Specifies the host location identifier.
	<b>none</b>	Specifies that no globally-defined location identifier is configured.
	<b>port-location</b>	(Optional) Defines port specific attributes.

**Command Default** The port location information of a civic location ID is not configured.

**Command Modes** Interface configuration (config-if)

Command History	Release	Modification
	15.1(1)SG	This command was introduced.
	15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

**Usage Guidelines** The **host** identifier configures the host civic location. If the identifier is not a host, the identifier only defines a civic location template that can be referenced on the interface. When you configure the **location civic-location-id host port-location** command, the command mode changes to civic location port configuration. The **host** keyword defines the device location. The civic location options available for configuration using *identifier*, **host**, and **none** are the same. You can specify the following civic location options for a port in civic location port configuration mode:

- **additional-code**--Sets an additional civic location code.
- **additional-location-information**--Sets additional civic location information.
- **branch-road-name**--Sets the branch road name.
- **building**--Sets building information.
- **city**--Sets the city name.
- **country**--Sets the two-letter ISO 3166 country code.
- **county**--Sets the county name.
- **default**--Sets a command to its defaults.
- **division**--Sets the city division name.

- **exit**--Exits from the civic location configuration mode.
- **floor**--Sets the floor number.
- **landmark**--Sets landmark information.
- **leading-street-dir**--Sets the leading street direction.
- **name**--Sets the resident name.
- **neighborhood**--Sets neighborhood information.
- **no**--Negates the specified civic location data and sets the default value.
- **number**--Sets the street number.
- **post-office-box**--Sets the post office box.
- **postal-code**--Sets the postal code.
- **postal-community-name**--Sets the postal community name.
- **primary-road-name**--Sets the primary road name.
- **road-section**--Sets the road section.
- **room**--Sets room information.
- **seat**--Sets seat information.
- **state**--Sets the state name.
- **street-group**--Sets the street group.
- **street-name-postmodifier**--Sets the street name postmodifier.
- **street-name-premodifier**--Sets the street name premodifier.
- **street-number-suffix**--Sets the street number suffix.
- **street-suffix**--Sets the street suffix.
- **sub-branch-road-name**--Sets the sub-branch road name.
- **trailing-street-suffix**--Sets the trailing street suffix.
- **type-of-place**--Sets the type of place.
- **unit**--Sets the unit.

## Examples

The following example shows how to configure the port location information of a civic ID in a device:

```
Device(config-if)# location civic-location-id host port-location
Device(config-if-port)# country US
Device(config-if-port)# building bg113
Device(config-if-port)# city Boston
Device(config-if-port)# state MA
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>location custom-location-id</b>	Configures the port location information of a custom location ID in a device.
<b>location geo-location identifier</b>	Configures the port location information of a geo-spatial location ID in a device.

## location custom-location identifier

To configure the custom location information of a host device, use the **location custom-location identifier** command in global configuration mode. To remove the custom location information, use the **no** form of this command.

**location custom-location identifier** {*identifier* | **host**}  
**no location custom-location identifier** {*identifier* | **host**}

### Syntax Description

<i>identifier</i>	Name of the custom identifier.
<b>host</b>	Defines the host custom location.

### Command Default

The custom location information of the host device is not configured.

### Command Modes

Global configuration (config)

### Command History

Release	Modification
15.1(1)SG	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

### Usage Guidelines

The **host** identifier configures the host custom location. If the identifier is not a host, the identifier only defines a custom location template that can be referenced on the interface. When you configure the **location custom-location identifier** *identifier* or **location custom-location identifier host** command on a device, the command mode changes to custom location configuration mode.

The **host** keyword defines the device location. The custom location options available for configuration using the *identifier* and the **host** keyword are the same.

You can specify the following custom location options in custom location configuration mode:

- **attribute**--Defines the attribute name and value
- **default**--Sets the location to its default attribute
- **exit**--Exits from custom location configuration mode
- **no**--Negates the specified attribute and sets the default attribute

The custom type data are exchanged with Cisco Discovery Protocol (CDP) using application programming interfaces (APIs). The custom type data following the **attribute** keyword is treated as opaque data and is used for description purpose. You can define multiple attribute value pairs within a custom location template. You can use the **show location custom-location identifier host** command to display the configured host custom location details.

### Examples

The following example shows how to configure custom location information for a device and how to define multiple attributes for a custom location:



```

Device(config)# location custom-location identifier host
Device(config-custom)# attribute bg115 "IDF 2.3"
Device(config-custom)# attribute mylabel "my location for this unit"
Device(config-custom)# attribute myotherlabel "something else"
Device(config-custom)# attribute Department "photography"
Device(config-custom)# attribute ParkingLot "10"

```

**Related Commands**

Command	Description
<b>location civic-location identifier</b>	Configures the civic location information of a device.
<b>location geo-location identifier</b>	Configures the geo-spatial location information of a device such as latitude, longitude, altitude, and resolution.
<b>show location custom-location identifier</b>	Displays the configured host custom location details.

## location custom-location-id

To configure the port location information of a custom location ID in a device, use the **location custom-location-id** command in interface configuration mode. To remove the location information, use the **no** form of this command.

```
location custom-location-id {identifier | host | none} [port-location]
no location custom-location-id {identifier | host | none} [port-location]
```

Syntax Description		
	<i>identifier</i>	Name of the custom identifier.
	<b>host</b>	Specifies the host location identifier.
	<b>none</b>	Specifies that no globally-defined location identifier is configured.
	<b>port-location</b>	(Optional) Specifies port specific attributes.

**Command Default** The port location of a custom location ID is not configured.

**Command Modes** Interface configuration (config-if)

Command History	Release	Modification
	15.1(1)SG	This command was introduced.
	15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

**Usage Guidelines** The **host** identifier configures the host custom location. If the identifier is not a host, the identifier only defines a custom location template that can be referenced on the interface. When you configure the **location custom-location-id host port-location** command, the command mode changes to port configuration mode. The **host** keyword defines the device location. The custom location options available for configuration under the *identifier*, the **host**, and the **none** are the same.

You can specify the following custom type data in port configuration mode:

- **attribute**--Defines the attribute name and value.
- **default**--Sets the location to its default attribute.
- **exit**--Exits from custom location configuration mode.
- **no**--Negates the specified attribute and sets the default attribute.

The custom type data are exchanged with Cisco Discovery Protocol (CDP) using application programming interfaces (APIs). The custom type data following the **attribute** keyword is treated as opaque data and is used for description purpose. You can define multiple attribute value pairs within a custom location template.

**Examples** The following example shows how to configure the port location information of a custom location ID in a device, and how to define multiple attributes for a custom location:

```
Device(config-if) # location custom-location-id host port-location  
Device(config-if-port) # attribute IDF 2.3
```

**Related Commands**

Command	Description
<b>location civic-location-id</b>	Configures the port location information of a civic location ID in a device.
<b>location geo-location-id</b>	Configures the port location information of a geo-spatial location ID in a device.

# location geo-location identifier

To configure the geo-spatial location information of a host device, use the **location geo-location identifier** command in global configuration mode. To remove the geographical location information, use the **no** form of this command.

```
location geo-location identifier {identifier | host}
no location geo-location identifier {identifier | host}
```

Syntax Description	
<i>identifier</i>	Name of the geographical identifier.
<b>host</b>	Defines the host geo-spatial location.

**Command Default** The geo-spatial location information of the host device is not configured.

**Command Modes** Global configuration (config)

Command History	Release	Modification
	15.1(1)SG	This command was introduced.
	15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

**Usage Guidelines** The **host** identifier configures the host geo-spatial location. If the identifier is not a host, the identifier only defines a geo-spatial location template that can be referenced on the interface. When you configure the **location geo-location identifier** *identifier* or **location geo-location identifier** **host** command on a device, the command mode changes to geo location configuration mode. The **host** keyword defines the device location. The geo-spatial options available for configuration under the *identifier* keyword and the **host** keyword are the same.

You can specify the following geo-spatial location information in geo location configuration mode:

- **altitude**--Sets altitude information in units of floor, meters, or feet.
- **latitude**--Sets latitude information in degrees, minutes, and seconds. The range is from -90 degrees to 90 degrees. Positive numbers indicate locations north of the equator.
- **longitude**--Sets longitude information in degrees, minutes, and seconds. The range is from -180 degrees to 180 degrees. Positive numbers indicate locations east of the prime meridian.
- **resolution**--Sets the resolution for latitude and longitude. If the resolution value is not specified, default value of 10 meters is applied to latitude and longitude resolution parameters. For latitude and longitude, the resolution unit is measured in meters. The resolution value can also be a fraction.
- **default**--Sets the geographical location to its default attribute.
- **exit**--Exits from geographical location configuration mode.
- **no**--Negates the specified geographical parameters and sets the default value.

You can use the **show location geo-location identifier** command to display the configured geo-spatial location details.

## Examples

The following example shows how to configure geo-spatial location information of a device:

```
Device(config)# location geo-location identifier host
Device(config-geo)# latitude 12.34
Device(config-geo)# longitude 37.23
Device(config-geo)# altitude 5 floor
Device(config-geo)# resolution 12.34
```

## Related Commands

Command	Description
<b>location civic-location identifier</b>	Configures the civic location information of a device.
<b>location custom-location identifier</b>	Configures the custom location information of a device.
<b>show location geo-location identifier</b>	Displays the configured geo-spatial location details.

# location geo-location-id

To configure the port location information of a geo-spatial location ID in a device, use the **location geo-location-id** command in interface configuration mode. To remove the geographical location information, use the **no** form of this command.

**location geo-location-id** {*identifier* | **host** | **none**} [**port-location**]  
**no location geo-location-id** {*identifier* | **host** | **none**} [**port-location**]

Syntax Description	
<i>identifier</i>	Name of the geo-spatial identifier.
<b>host</b>	Specifies the host location identifier.
<b>none</b>	Specifies that no globally-defined location identifier is configured.
<b>port-location</b>	(Optional) Defines port specific attributes.

**Command Default** The port location information of a geo-spatial location ID is not configured.

**Command Modes** Interface configuration (config-if)

Command History	Release	Modification
	15.1(1)SG	This command was introduced.
	15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

**Usage Guidelines** The **host** identifier configures the host geo-spatial location. If the identifier is not a host, the identifier only defines a geo-spatial location template that can be referenced on the interface. When you configure the **location geo-location-id host port-location** command, the command mode changes to port configuration mode.

The **host** keyword defines the device location. The geo-spatial location options available for configuration under *identifier*, **host**, and **none** are the same.

You can specify the following geo-spatial location details in port location configuration mode:

- **altitude**--Sets altitude information in units of floor, meters, or feet.
- **latitude**--Sets latitude information in degrees, minutes, and seconds. The range is from -90 degrees to 90 degrees. Positive numbers indicate locations north of the equator.
- **longitude**--Sets longitude information in degrees, minutes, and seconds. The range is from -180 degrees to 180 degrees. Positive numbers indicate locations east of the prime meridian.
- **resolution**--Sets the resolution for latitude and longitude. If the resolution value is not specified, default value of 10 meters is applied to the latitude and longitude resolution parameters. For latitude and longitude, the resolution unit is measured in meters. The resolution value can also be a fraction.
- **default**--Sets the geographical location to its default attribute.
- **exit**--Exits from geographical location configuration mode.

- **no**--Negates the specified geographical parameters and sets the default value.

### Examples

The following example shows how to configure the port location information of a geo-spatial location in a device:

```
Device(config-if) # location geo-location-id host port-location
Device(config-if-port) # latitude 12.34
Device(config-if-port) # longitude 37.23
Device(config-if-port) # altitude 5 floor
Device(config-if-port) # resolution 12.34
```

### Related Commands

Command	Description
<b>location civic-location-id</b>	Configures the port location information of a civic location ID in a device.
<b>location custom-location-id</b>	Configures the port location information of a custom location ID in a device.

# location prefer

To assign a priority for location information on Cisco Discovery Protocol (CDP) messages, use the **location prefer** command in global configuration mode. To disable the priorities assigned to location information on CDP messages, use the **no** form of this command.

**location prefer** {**cdp** | **lldp-med** | **static**} **weight** *priority-value*  
**no location prefer** {**cdp** | **lldp-med** | **static**} **weight** *priority-value*

Syntax Description	Parameter	Description
	<b>cdp</b>	Specifies the priority for CDP.
	<b>lldp-med</b>	Specifies the priority for Link-Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) protocol.
	<b>static</b>	Specifies static location information.
	<b>weight</b>	Specifies the priority for the specified protocol or static location information.
	<i>priority-value</i>	Priority value. The range is from 0 to 255.

**Command Default** The static location information has the highest priority, followed by CDP and LLDP.

**Command Modes** Global configuration (config)

Command History	Release	Modification
	12.2(55)SE	This command was introduced.
	15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

**Usage Guidelines** Location information can either be configured statically or updated dynamically. The location database is populated with the location information that you configure from various modules, such as CDP and LLDP. If the same information is available on multiple modules, the device picks up one source based on the priority configured using the **location prefer** command. Use the **weight** keyword to configure the priority of the location information. A lower numerical value specified for the *priority-value* argument indicates a higher priority.

**Examples** The following example shows how to configure the location information priority for CDP messages:

```
Device(config)# location prefer cdp weight 10
```

Related Commands	Command	Description
	<b>location</b>	Configures location information for an endpoint.
	<b>location (interface)</b>	Configures location information for an interface.



# show-macsec-post

To verify the macsec Power on Self Test (POST) configuration, use the **show macsec post** command in privileged EXEC mode.

## show macsec post

### Command Default

The command is enabled.

### Command Mode

Privileged EXEC

### Example

To verify the macsec Power on Self Test (POST) configuration:

```

MACsec Capable Interface                                POST Result
-----
GigabitEthernet0/1/0                                  PASS
GigabitEthernet0/1/2                                  PASS
GigabitEthernet0/1/4                                  PASS
GigabitEthernet0/1/6                                  PASS
GigabitEthernet0/1/8                                  NONE
GigabitEthernet0/1/10                                 NONE
GigabitEthernet0/1/12                                 NONE
GigabitEthernet0/1/14                                 NONE
TenGigabitEthernet0/1/16                              PASS
GigabitEthernet0/2/0                                  PASS
GigabitEthernet0/2/2                                  PASS
GigabitEthernet0/2/4                                  PASS
GigabitEthernet0/2/6                                  NONE

```

### Command History

Release	Modification
Cisco IOS XE Cupertino 17.8.1	The command was introduced for ASR 900 and NCS 4206 Cisco RSP3 module.

